Symantec™ IT Management Suite 7.5 powered by Altiris™ – Planungs- und Implementierungshandbuch

Symantec

Symantec™ IT Management Suite powered by Altiris™ – Planungs- und Implementierungshandbuch

Die in diesem Handbuch beschriebene Software wird unter einer Lizenzvereinbarung zur Verfügung gestellt und darf nur gemäß den Bestimmungen dieser Vereinbarung verwendet werden.

Rechtlicher Hinweis

Copyright © 2013 Symantec Corporation. Alle Rechte vorbehalten.

Symantec, das Symantec-Logo, das Häkchen-Logo und alle im Produkt verwendeten Marken von Altiris oder Symantec sind Marken oder eingetragene Marken der Symantec Corporation oder ihrer verbundenen Unternehmen in den USA und anderen Ländern. Andere Bezeichnungen können Marken anderer Rechteinhaber sein.

Dieses Symantec-Produkt kann Drittanbietersoftware enthalten, für die Symantec die Rechte der Drittanbieter ("Nicht-Symantec-Programme") anerkennt. Einige Nicht-Symantec-Programme sind als "open source" oder als freie Softwarelizenzen verfügbar. Die Lizenzvereinbarungen dieser Software haben keine Auswirkungen auf die Rechte oder Verpflichtungen, die Ihnen unter den "open source" oder freien Softwarelizenzen möglicherweise zustehen. Weitere Informationen finden Sie im Anhang mit rechtlichen Hinweisen zu Nicht-Symantec-Programmen in dieser Dokumentation oder in der TPIP-Readme-Datei dieses Symantec-Produkts.

Das in diesem Dokument beschriebene Produkt wird unter Lizenzen vertrieben, die die Nutzung, Vervielfältigung, Verteilung und Dekompilierung/Zurückentwicklung (reverse engineering) einschränken. Ohne vorherige schriftliche Genehmigung der Symantec Corporation oder ihrer Lizenzgeber (falls zutreffend) darf kein Teil dieses Dokuments vervielfältigt werden, unabhängig davon, in welcher Form oder mit welchen Mitteln dies geschieht.

DIE DOKUMENTATION WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT. ALLE AUSDRÜCKLICHEN UND STILLSCHWEIGENDEN VORAUSSETZUNGEN, DARSTELLUNGEN UND GEWÄHRLEISTUNGEN, EINSCHLIESSLICH DER STILLSCHWEIGENDEN GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER NICHT-BEEINTRÄCHTIGUNG, SIND AUSGESCHLOSSEN, AUSSER IN DEM UMFANG, IN DEM SOLCHE HAFTUNGSAUSSCHLÜSSE ALS NICHT RECHTSGÜLTIG ANGESEHEN WERDEN. SYMANTEC CORPORATION IST NICHT VERANTWORTLICH FÜR INDIREKTE SCHÄDEN ODER FOLGESCHÄDEN IM ZUSAMMENHANG MIT DER BEREITSTELLUNG ODER VERWENDUNG DIESER DOKUMENTATION. DIE IN DIESER DOKUMENTATION ENTHALTENEN INFORMATIONEN KÖNNEN JEDERZEIT OHNE ANKÜNDIGUNG GEÄNDERT WERDEN.

Die lizenzierte Software und Dokumentation gelten als kommerzielle Computersoftware gemäß FAR 12.212 und unterliegen den eingeschränkten Rechten gemäß FAR, Abschnitt 52.227-19 "Commercial Computer Software - Restricted Rights" und DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation" und einschlägigen Folgebestimmungen. Jede Verwendung, Modifikation, Reproduktionsversion,

Vorführung, Vorstellung oder Offenlegung der lizenzierten Software und Dokumentation seitens der US-amerikanischen Regierung darf ausschließlich in Übereinstimmung mit den Bestimmungen dieser Vereinbarung erfolgen.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.de

Technischer Support

Der technische Support von Symantec betreibt weltweit Supportcenter. Die Hauptfunktion des technischen Supports ist die Bearbeitung spezifischer Anfragen zu Produkteigenschaften und -funktionen. Außerdem erstellt der technische Support Inhalte für die Online-Supportdatenbank. Die Gruppen des technischen Supports arbeiten eng mit anderen Bereichen von Symantec zusammen, um Ihre Fragen zeitgerecht zu beantworten. So arbeiten beispielsweise die Gruppen des technischen Supports mit den Entwicklungsingenieuren und dem Symantec Security Response-Team zusammen, um Warnungen und aktualisierte Virendefinitionen bereitzustellen.

Das Supportangebot von Symantec beinhaltet Folgendes:

- Verschiedene Supportoptionen mit der nötigen Service-Flexibilität für Organisationen aller Größen
- Telefon- und/oder webbasierter Support mit schnellen Reaktionszeiten und Informationen auf dem allerneuesten Stand
- Sicherstellung von Upgrades zur Bereitstellung von Software-Upgrades
- Globaler Support, der basierend auf lokalen Geschäftszeiten oder 24-Stunden-Support an 7 Tagen in der Woche erworben wurde
- Premium-Serviceangebote, die Account Management-Services umfassen

Ausführliche Informationen zu den Supportangeboten von Symantec finden Sie auf unserer Website unter der folgenden URL:

www.symantec.com/business/support/

Alle Support-Services werden entsprechend Ihrer Supportvereinbarung und den zum gegebenen Zeitpunkt aktuellen technischen Supportrichtlinien des Unternehmens bereitgestellt.

Kontaktieren des technischen Supports

Kunden mit einem aktuellen Supportvertrag können auf Informationen des technischen Supports unter folgender URL zugreifen:

www.symantec.com/de/de/business/support/

Bevor Sie den technischen Support kontaktieren, stellen Sie sicher, dass die Systemanforderungen erfüllt sind, die in Ihrer Produktdokumentation aufgelistet sind. Auch sollten Sie sich an dem Computer befinden, auf dem das Problem aufgetreten ist, falls eine Replizierung des Problems notwendig ist.

Wenn Sie den technischen Support kontaktieren, halten Sie bitte die folgenden Informationen bereit:

- Produktversion
- Hardware-Daten
- Verfügbarer Arbeitsspeicher, Speicherplatz und NIC-Informationen
- Betriebssystem
- Version und Patch-Level
- Netzwerktopologie
- Informationen zu Router, Gateway und IP-Adressen
- Problembeschreibung:
  - Fehlermeldungen und Protokolldateien
  - Fehlerbehebungsmaßnahmen, die vor Kontaktaufnahme mit Symantec durchgeführt wurden
  - Aktuelle Softwarekonfigurationsänderungen und Netzwerkänderungen

Lizenzierung und Registrierung

Wenn Ihr Symantec-Produkt eine Registrierung oder einen Lizenzschlüssel erfordert, besuchen Sie unsere technische Support-Webseite:

www.symantec.com/de/de/business/support/

Kundenservice

Informationen zum Kundenservice finden Sie unter folgender URL:

www.symantec.com/de/de/business/support/

Der Kundenservice kann bei nicht-technischen Fragen helfen. Beispiele:

- Fragen zu Produktlizenzen und -seriennummern
- Aktualisieren persönlicher Angaben wie Anschrift und Name
- Allgemeine Produktinformationen (Funktionen, verfügbare Sprachen, lokale Anbieter)
- Neueste Informationen zu Produkt-Updates und -Upgrades
- Informationen zu Upgrade-Versicherung und Support-Verträgen
- Informationen zum Symantec Buying Program
- Informationen zu den Optionen des technischen Support von Symantec
- Nichttechnische Fragen zu vertriebsvorbereitenden Maßnahmen
- Probleme mit CDs, DVDs oder Handbüchern

Ressourcen zum Supportvertrag

Wenn Sie Symantec bezüglich eines vorhandenen Supportvertrags kontaktieren möchten, wenden Sie sich bitte an das Supportvertragsverwaltungsteam für Ihre Region:

Asien-Pazifik und Japan	customercare_apac@symantec.com
Europa, Nahost und Afrika	semea@symantec.com
Nordamerika und Lateinamerika	supportsolutions@symantec.com

Inhalt

Technischer Support 4

Kapitel 1 Einführung in IT Management Suite 11

Informationen zur IT Management Suite 11
Funktionen der IT Management Suite 12
Funktionsweise der IT Management Suite 13
Weitere Informationen 18

Kapitel 2 Die Komponenten von IT Management Suite 21

Info zur Symantec Management-Plattform 21
Architekturkomponenten von Symantec Management-Plattform 22
Komponenten der Symantec Management-Plattform 23
Lösungen der IT Management Suite 24
Info zu Cloud-fähiger Verwaltung 31
Bereitstellen von Software mithilfe von Deployment Solution 33

Kapitel 3 Planung für IT Management Suite 37

Überlegungen zu Planung der IT-Verwaltung 37
Informationen zur Planung Ihrer SQL Server-Konfiguration 39
Info zur Festplattenkonfiguration für SQL Server 41
Informationen über die Festlegung der Datenbankgröße für SQL Server 42
Info zur Arbeitsspeicherverwaltung für SQL Server 43
Informationen zur Verwaltung der SQL-Datenbank 45
Verwenden des Microsoft SQL-Failover-Clustering mit ITMS 7.1 SP2 oder höher 46
Informationen zur Planung Ihrer Site Server 51
So planen Sie ein Site-Design 51
Info zur Site-Verwaltung 52
Informationen zum Task Service 53
Wie Task Server die Tickle-Funktion verwendet 55
Informationen zum Paketdienst 57
Info zum Netzwerkstartdienst 58
Symantec Management Agent-Bereitstellungsplanung 60

Info zu Agent-Registrierung 61

Kapitel 4 Hardwareempfehlungen 62

Empfohlene Hardware für die IT Management Suite 7.5 62
Empfohlene Internet-Gateway-Hardware 66
Empfohlene Konfiguration für Notification Server mit lokal installierter SQL-Datenbank 67
Empfohlene maximale Computeranzahl für IT Management Suite 7.5 68
Unterstützte Betriebssysteme für Notification Server und Site Server 69
Info zu unterstützten SQL Server-Kollatierungen 72
Durch Symantec Installation Manager installierte IIS Rollen-Dienste 73
SQL Server-Empfehlungen und Drittanbietersoftware-Anforderungen 75

Kapitel 5 Lösungskommunikationen 77

Funktionsweise der Aufgaben in Deployment Solution 77
Wie Agent-Check-in-Intervalle und Grundinventareinstellungen kommunizieren 78
Vorgehensweise bei der agentenbasierten Übermittlung von Inventardaten 78
Info zum Konfigurieren von Inventarisierungsrichtlinien- und Aufgabeneinstellungen zur optimalen Ressourcennutzung 81
Methoden zum Erfassen von Inventardaten 86
Info zur Paketverteilung in einer Hierarchie 92
Funktionsweise des Patch Management Solution-Datenaustauschs 95
Datenaustausch in der Asset Management Suite 99
Auswählen einer Methode für Software Delivery 100
Informationen zu Erkennungsregeln 102
Erstellen einer Erkennungsregel 103
Softwareportal einrichten 105

Kapitel 6 Empfehlungen zum Feinabstimmen und Optimieren der Leistung 107

Info zum Bestimmen, ob Sie eine Leistungsoptimierung benötigen 107
Leistungsfaktoren der Symantec Management-Plattform 108

Informationen zur Leistungsoptimierung der Notification Server-Ereignisverarbeitung 109
Info zu vordefinierten Inventarisierungsrichtlinien 110
Planen von Ressourcen-Mitgliedschaftsaktualisierungen 111
Informationen über die Leistungsoptimierung des Symantec Management Agents 113
Empfohlene Konfigurationseinstellungen basierend auf verwalteten Endgeräten 115
Informationen zur Leistungsverbesserung der Symantec Management-Plattform-Konsole 116

Kapitel 7 Umgebungen mit mehreren Notification Servers 117

Replikationstypen der Symantec Management-Plattform 117
Info zur Hierarchiereplikation 118
Einsatzmöglichkeiten der Hierarchiereplikation 120
Info zur Hierarchietopologie 120
So funktionieren Site Server in einer Hierarchie 121
Überlegungen zur Implementierung der Hierarchiereplikation für Software Management Solution 121
Überlegungen zur Implementierung der Hierarchiereplikation für Patch Management Solution 122
Einschränkungen der Hierarchiereplikation 122
Implementieren der Notification Server-Hierarchie 124
Info zu Peer-zu-Peer-Replikation und Replikationsregeln 126
Informationen zur MultiCMDB-Berichtserstellung mit IT Analytics 128

Anhang A Symantec IT Management Suite – Plattformunterstützungsmatrix 130

Einleitung 130
Symantec Management-Plattform 131
Notification Server und Workflow-Server 131
Microsoft SQL Server 133
Microsoft SQL Server Collations 134
Microsoft IIS 135
Microsoft .NET 135
Konsole/Browser 136
Workflow Designer 137
Site Server 138
Cloud-fähige Verwaltung (bisher IBCM) 142
Client Management Suite 143

Client-Betriebssystemunterstützung 143
Server Management Suite 148
Server-Betriebssystemunterstützung 149
Deployment Solution 155
Sprachunterstützung 164
Core-Lokalisierung 164
Windows-Agent-Lokalisierung 165

Index 166

Kapitel 1

Einführung in IT Management Suite

In diesem Kapitel werden folgende Themen behandelt:

- Informationen zur IT Management Suite
- Funktionen der IT Management Suite
- Funktionsweise der IT Management Suite
- Weitere Informationen

Informationen zur IT Management Suite

Die IT Management Suite (ITMS) kombiniert die Client- und Server-Konfigurationsverwaltung mit der IT-Ressourcen- und Diensterwaltung. Sie fördert die effektive Service-Bereitstellung und unterstützt die Kostenreduzierung und die Komplexität der Verwaltung von Unternehmens-IT-Ressourcen. Diese Assets umfassen möglicherweise Desktops, Laptops, Thin Clients und Server in den heterogenen Umgebungen, auf denen Windows, Linux, UNIX und Mac ausgeführt werden. Sie können alle Funktionen der Suite über eine zentrale Konsole auf einer gemeinsamen Plattform verwalten: die Symantec Management-Plattform. Diese gemeinsame Plattform integriert Verwaltungsfunktionen, um die Automatisierung für einen besseren Service, eine höhere Wertschöpfung und IT-Effizienz zu beschleunigen.

Siehe "Funktionen der IT Management Suite" auf Seite 12.

IT Management Suite enthält folgende Verwaltungsfunktionen:

- Server Management
  Server Management enthält eine Vielzahl von Assistenten und anderen Funktionen, mit denen Sie zur Verwaltung Ihrer Server die Konfiguration

automatisieren, Aufgaben bereitstellen und Richtlinien erstellen können. Die Serververwaltungsfunktionen unterstützen Windows, UNIX und Linux. Darüber hinaus werden die gleichen Verwaltungsdisziplinen sowohl auf die physischen Systeme als auch auf die virtuellen Systeme angewendet, einschließlich Microsoft Hyper-V und VMware.

- Clientverwaltung
  Die Clientverwaltung hilft bei der Erkennung von Ressourcen in Ihrem Netzwerk und ermöglicht die Überprüfung ihres Status. Die Berichterstellungstools helfen Ihnen, Probleme zu identifizieren und unmittelbar zu beheben. Die Funktionen der Clientverwaltung unterstützen Windows, Linux und Mac.
- IT-Ressourcenverwaltung
  Die IT-Ressourcenverwaltung baut auf eine solide Inventargrundlage für die Konfigurationsverwaltung auf. Sie unterstützt Sie darin, die zu erkennenden und nicht zu erkennenden Ressourcen zu bewerten und Ihre Ressourcen und ressourcenbezogenen Informationen nachzuverfolgen. Sie können Verträge, Softwarelizenz-Richtlinieneinhaltung und Beschaffungsprozesse sowie die Konfigurationselemente verwalten, die Ihren Ressourcen zugeordnet sind.

Siehe "Funktionen der IT Management Suite" auf Seite 12.

Siehe "Funktionsweise der IT Management Suite" auf Seite 13.

Funktionen der IT Management Suite

Mit der IT Management Suite (ITMS) können Sie die Service-Bereitstellung verbessern, die Effizienz steigern und Kosten reduzieren.

Sie können mit der IT Management Suite folgende Schritte durchführen:

- Über eine zentrale Konsole verwalten.
  Sie können heterogene Client- und Server-Endgeräte zentral verwalten.
- Verwalten über Fernzugriff.
  Mit 1:1-Remote-Verwaltungsfunktionen können Sie Eingriffe am Arbeitsplatz oder auf dem Server vermeiden.
- Automatisieren von Aufgaben.
  Mit der Task-Engine können Sie mehrere Remote-Verwaltungsaufgaben gleichzeitig durchführen.
- Automatisieren der Richtliniendurchsetzung.
  Mit der Richtlinien-Engine können Sie automatisch erkennen und bereinigen, ohne menschlichen Eingriff.
- Automatisieren von Prozessen.

Mit der Workflow-Engine können Sie menschliche und Systeminteraktionen automatisieren, um Zugriffsverzögerungsfehler und -auslassungen zu beseitigen.

- Erstellen der Selbstbedienung.
  Mit dem Dienstkatalog können Sie Anrufe oder Anfragen mit der bewährten Selbsthilfe vermeiden.
- Software zentral verwalten.
  Software-Verwaltung umfasst Softwareinventarisierung, Patchen, Lieferung und Lizenzverwaltung.

Siehe "Informationen zur IT Management Suite" auf Seite 11.

Funktionsweise der IT Management Suite

IT Management Suite (ITMS) ist ein Bündel von Symantec-Produkten und -Software. IT Management Suite unterstützt Sie bei der Bereitstellung, der Verwaltung, dem Support und der Deaktivierung der verschiedenen Computer, Geräte, Server und IT-Ressourcen in Ihrem Unternehmen. IT Management Suite beinhaltet die Verwaltung von IT-Ressourcen sowie die Verwaltung von Client- und Server-Konfigurationen.

Siehe "Informationen zur IT Management Suite" auf Seite 11.

IT Management Suite hat folgende Hauptmerkmale und -funktionen:

- Zentrale Management-Plattform
  Alle Teile der IT Management Suite werden auf einer gemeinsamen Grundlage erstellt, die Symantec Management-Plattform genannt wird. Die Symantec Management-Plattform ist ein Satz Kerndienstleistungen, die alle Teile der IT Management Suite gemeinsam haben. Diese Dienstleistungen können Aspekte, wie Sicherheit, Berichterstellung, Kommunikation und Datenspeicherimg umfassen.
  IT Management Suite bietet eine verbesserte Verwaltungsoberfläche, mit der Sie schneller ihre Ziele erreichen. Gemeinsamen Konzepte, wie Computerverwaltung, Softwarebereitstellung und Lizenzverwaltung und -bereitstellung stellen jetzt eine integrierte Erfahrung dar. Wenn Sie auf auf einen Computer klicken, sind die Ressourcenverwaltungsdetails sofort sichtbar. Leistungsstarke Suchfunktionen unterstützen Sie darin, einen Drilldown durchzuführen und in kurzer Zeit Filter zu erstellen. Sie können die Suchen schnell für die künftige Nutzung speichern. Mit den Drag-and-drop-Funktionen können Sie Aufgaben auswählen und sie auf einen oder mehrere ausgewählte Computer ziehen.
- Gemeinsame Datenbank und Verwaltungskonsole

Die verschiedenen Teile der Plattform können von einer gemeinsamen Datenbank gelesen und geschrieben werden. Die Datenbank wird Configuration Management Database (CMDB) genannt. Obwohl IT Management Suite eine Vielzahl von IT-bezogenen Funktionen beinhaltet, sind alle Technologien über eine gemeinsame webbasierte Benutzeroberfläche abrufbar. Diese Schnittstelle ist die Symantec Management Console.

- Management-Agent und Management-Server
  IT Management Suite kann die Computer erkennen, die in Ihrer Umgebung vorhanden sind. Sie können Symantec Management Agent auf diesen Computern installieren. Der Agent ermöglicht Ihnen das Zusammentragen ausführlicher Informationen über sie. Er sendet regelmäßig Informationen über den Computer an einen Management-Server-Computer namens Notification Server. Notification Server verarbeitet die Informationen über Ihre Computer und speichert sie in einer gemeinsamen Datenbank. Symantec Management-Agent bietet Ihnen eine robuste Steuerung und Einblick in die Hardware und die Software auf Ihren verwalteten Computern und Servern. Es hilft Ihnen, Ihre Unternehmensstandards und -richtlinien von der webbasierten Symantec Management Console über Fernzugriff beizubehalten.
- Asset-Verwaltung
  Sie können die Daten in CMDB verwenden, um Ihre Ressourcen leistungsfähiger zu verwalten. Beispielsweise können Sie diese Informationen mit Berichten und Filtern verwenden, um Einblick in und Metriken über die Ressourcen in Ihrer Umgebung zu erhalten
- Lizenzverwaltung
  Lizenzverwaltung und Ressourcenverwaltung sowie Verwendung sind fest integriert. Innerhalb der Software-Anzeige befindet sich eine Übersichtsansicht der aktuellen Bereitstellungen und der Kostendetails. Diese Details basieren auf den aktuellen Installationen und den Kaufdetails. Anhand einer Grafik können Sie ermitteln, ob ein Softwareprodukt zu häufig oder zu wenig häufig verteilt ist, und seine aktuelle Nutzung auswerten. Sie bietet eine Übersicht über die finanziellen Auswirkungen eines Produkts. Sie können die potenziellen Einsparungen des Sammelns von Lizenzen sehen, und Sie können die Kostenauswirkung sehen, wenn ein Produkt zu sehr verteilt ist.
- Software Management
  Sie können sehen, welche Software installiert ist, wie häufig sie verwendet wird und wie viele Lizenzen Sie für sie erworben haben. Dieser Typ von Informationen kann Ihnen helfen, zu bestimmen, welche IT-Ressourcen Sie erwerben müssen. Sie können diese Informationen auch verwenden, um zu bestimmen, wie Ihre Software-Investition maximiert und wann die Software ersetzt oder stillgelegt wird. Darüber hinaus können Sie die IT Management Suite verwenden, um bezüglich der Informationen, die sie zusammenträgt, aktiv zu werden.

Beispielsweise erkennt IT Management Suite möglicherweise, dass bestimmte Software installiert und lizenziert ist, jedoch nicht verwendet wird. Sie können die Suite so konfigurieren, dass die unbenutzte Software entfernt wird.

In IT Management Suite wird die Softwarekatalogschnittstelle optimiert und neu entworfen. Jede mögliche Software, die gefunden wird, wird in der eben erkannten Liste gespeichert. Anhand dieser Liste können Sie schnell erkennen, ob die identifizierte Software ein verwaltetes Produkt sein soll. Ist dies nicht der Fall, können Sie sie nicht verwalteter Software zuweisen. Nachdem Sie Software als verwaltetes Softwareprodukt identifiziert haben, können Sie alle Elemente in einer einzigen Oberfläche verwalten. Sämltiche Inventar-, Mess., Lieferungs- und Lizenznachverfolgungen werden in nur einer Oberfläche dargestellt.

Die Funktion für die kontrollierte Verteilung trennt jetzt den Zeitplan für Lieferung und Ausführung. Sie können Pakete im Voraus bereitstellen, und dann später die Ausführung planen.

- Aufgabe- und Richtlinien-Engines

  Notification Server hat zwei Komponenten, die als Task-Engine und Richtlinien-Engine bezeichnet werden. Mit diesen Komponenten können Sie auf Ihren verwalteten Computern arbeiten. Sie können Richtlinien verwenden, um konsistente Standards beizubehalten, und Sie können Aufgaben verwenden, um sequenzielle Schritte auszuführen. Richtlinienbasierte Verwaltung kann die Autonomie des verwalteten Computers ermöglichen, unabängig davon, ob er sich in einem verbundenen oder nicht verbundenen Zustand befindet. Aufgabengestützte Verwaltung folgt dem traditionellen Server-zu-Client-Kommunikationsparadigma.

- Verwaltete Computer

  Auf verwalteten Computern ist der Management-Agent installiert. Sie kommunizieren regelmäßig mit dem Notification Server-Computer. Wenn ein verwalteter Computer Notification Server kontaktiert, prüft er, ob Sie für ihn Arbeit konfiguriert haben.

  Der Agent kann prüfen, ob der Computer, auf dem er installiert ist, mit einer Richtlinie kompatibel ist. Beispielsweise können Sie eine Richtlinie einrichten, um sicherzustellen, dass alle Ihre verwalteten Computer die neueste Version der Software aufweisen. Wenn sie nicht kompatibel ist, dann kann der Agent die Software entsprechend Ihren Einstellungen herunterladen und installieren. Wenn Software über Remote-Zugriff auf Zielcomputern mit Notification Server ausgeführt wird, wird diese Software ein Softwarepaket genannt.

- Patch-Verwaltung

  Sie können IT Management Suite verwenden, um Ihre Computer sicher, gepatcht und kompatibel zu machen. Mit der IT Management Suite können Sie alle Aspekte von Microsoft Windows-Sicherheits-Updates und -Patches verwalten.

- Bereitstellung

Sie können standardisierte Betriebssystem-Images auf Ihre Computer über Remote-Zugriff bereitstellen und verteilen. Diese Funktionalität umfasst die Bereitstellung auf bloßer Metall-Hardware und das erneute Imaging von Computern, um sie in einen bekannten guten Zustand zurück zu versetzen.

- Migration und Bereitstellung
  Deployment Solution ist systemeigen in die Symantec Management-Plattform integriert. Infolgedessen arbeiten Sie mit Deployment Solution und der Symantec Management-Plattform über eine einzelne Konsole, eine Datenbank und einen Agent. IT Management Suite stellt viele Verbesserungen zur Deployment Solution-Konsole zur Verfügung.
  Die "DeployAnywhere"-Funktion unterstützt alle bedienungsfertigen Treibertypen für Hardware-unabhängiges Imaging. Diese Zusatzfunktion ergänzt den Support, damit Hardwareabstraktions-Layer (HAL), Netzwerkkarten und Controllertreiber für Massenspeicher eine vollständige Hardware-unabhängige Imaging-Lösung zur Verfügung stellen. Die Verwaltung für die Treiberdatenbank ist jetzt über die Konsole verfügbar. Sie können die Treiberverwaltung konsolidieren, weil sowohl das Imaging als auch die skriptgesteuerten Betriebssysteminstallationen die Treiber in der "DeployAnywhere"-Datenbank nutzen.
  Ghost-Imaging unterstützt das vertraute RapiDeploy-Multicasting. PC Transplant unterstützt Microsoft Office 2010 (32-Bit und 64-Bit).
  Erweiterte Virtual Machine Management-Funktionen strukturieren die Konfiguration und erweitern den Erstellungsassistenten des virtuellen Rechners. Der Assistent kann jeden Deployment Solution-Job als Teil des Erstellungsprozesses des virtuellen Rechners ausführen. Mit dieser Funktion können Sie vorhandene Serverbereitstellungs-Jobs nutzen und sie für die Bereitstellung des virtuellen Servers anwenden.
- Überwachung des Serverzustands
  Mit der IT Management Suite können Sie auch den Zustand Ihrer Server überwachen und beibehalten. Sie können wichtige Metriken und Anzeigen Ihrer Serverzustandsleistung überwachen. Diese Metriken können in Echtzeit angezeigt werden. Mit der Task-Engine können Sie Ihre Server proaktiv verwalten. Beispielsweise können Sie komplexe Folgen von den Failsafemaßnahmen, wie zum Beispiel die Bereitstellung eines Backup-Servers im Falle eines Serverabsturzes automatisieren. Sie können das System so konfigurieren, dass Sie alarmiert werden, wenn eine bestimmte Metrik auf ein potenzielles Problem hinweist. Sie können dieses Problem dann so lösen, dass es in Zukunft nicht mehr auftritt.
- Workflow-Engine
  Die IT-Verwaltung enthält eine Workflow-Engine, mit der Sie menschliche und Systeminteraktionen automatisieren können. Sie können robuste Arbeitsabläufe

einrichten, um viele der sequenziellen Aufgaben automatisch abzuschließen, die für eine leistungsfähige Dienstverwaltung erforderlich sind.

Zusätzlich zu den Formulararerstellungs- und Drag & Dop-Designerfunktionen können Sie die vollständige Komponentengeneratorfunktion für den Zugriff auf Technologien von Drittanbietern verwenden. Diese Technologien umfassen "HR" oder Finanzsysteme und das Portal "Workflow". Mit dem Portal "Workflow" können Sie den Gesamtprozess nachverfolgen, wenn ein Workflow die verschiedenen Stadien durchläuft.

- Erweiterte Berichterstellung und IT Analytics

  Das Executivdashboard und die Trendanalyse bieten Ihnen eine repräsentative Ansicht Ihrer IT-Ressourcen. Mit den Schlüsselleistungsanzeigen können Sie kritische Erfolgsfaktoren für Ihre Organisation messen und schnell Tendenzen auswerten, wie sich diese Maßnahmen im Laufe der Zeit ändern. Sie können Ad-hoc-Data-Mining verwenden, um Pivot-Tabellenansichten zu bilden. Die Berichte basieren auf vordefinierten Maßnahmen und Abmessungen. Die Funktionalität ermöglicht eine einfache Bearbeitung der Daten, damit Sie kein SQL-Experte sein müssen, um auf die benötigten Informationen zuzugreifen. Mehrdimensionale Analyse und robuste grafische Berichterstellung sind enthalten, damit Sie Ihre Antworten mit sehr wenig Anpassung und ohne Wartezeit erhalten.

  Die MultiCMDB-Funktion bietet eine globale IT Analytics-Berichterstellung über mehrere CMDBs hinweg, ohne die Notwendigkeit, große Datenmengen zu replizieren.

- Symantec Workspace Virtualization

  Eine Schlüsselherausforderung für den Übergang zu Windows 7 besteht darin, dass viele veraltete Internetanwendungen von Internet Explorer 6 abhängig sind. Symantec Workspace Virtualization bietet ein neues Update, das dieses Problem löst. Sie können Internet Explorer 6 direkt in Windows 7 virtualisieren. Dadurch ist die gleichzeitige Ausführung von Internet Explorer 6, 7 und 8 möglich. Sie können auch mehrere Java-Versionen auf dem systemeigenen Betriebssystem ausführen, um normale Ansichten zu haben.

  Mit diesem Ansatz sind die Nutzung nebeneinander sowie die sichere Implementierung möglich, die für den Benutzer unsichtbar ist. Sie können festlegen, welche Anwendungen Zugriff auf diesen speziellen Browser haben sollen. Die Benutzer werden nie aufgefordert, einen Browser auszuwählen. Die richtige Version wird automatisch basierend auf der Richtlinie geöffnet. Mit dieser Option können Sie schneller und effizienter zu Microsoft Windows 7 migrieren. Browser-Plugins, wie zum Beispiel Acrobat und Flash können an der Basis oder in einem virtuellen Layer installiert werden. Mehrere Java-Versionen können an der Basis oder in einem Layer installiert werden, und durch einen virtuellen Internet Explorer verwendet werden. Workspace Virtualization unterstützt alle

Gruppenrichtlinienobjekte automatisch, die Ihr Unternehmen möglicherweise für Internet Explorer zur Verfügung stellt.

Siehe "Funktionen der IT Management Suite" auf Seite 12.

Weitere Informationen

Machen Sie sich anhand der folgenden Dokumentationsressourcen mit der Verwendung des Produkts vertraut.

Tabelle 1-1 Dokumentationsressourcen

Dokument	Beschreibung	Speicherort
Versionshinweise	Informationen über neue Funktionen und wichtige Themen.	Die Seite "Unterstützte Produkte A-Z" ist unter folgender URL verfügbar: http://www.symantec.com/business/support/index?page=products Öffnen Sie die Supportseite Ihres Produkts und klicken Sie dann unter "Allgemeine Themen" auf "Versionshinweise".
Implementierungshandbuch	Informationen zur Installation, Konfiguration und Implementierung dieses Produkts.	■ Die Dokumentationsbibliothek ist in der Symantec Management Console im Menü "Hilfe" verfügbar. ■ Die Seite "Unterstützte Produkte von A-Z" ist unter folgender URL verfügbar: http://www.symantec.com/business/support/index?page=products Öffnen Sie die Supportseite Ihres Produkts und klicken Sie dann unter "Allgemeine Themen" auf "Dokumentation".
Benutzerhandbuch	Informationen zur Verwendung dieses Produkts, einschließlich detaillierter technischer Informationen und Anweisungen zur Ausführung von Routineaufgaben.	■ Die Dokumentationsbibliothek ist in der "Symantec Management Console" im Menü Hilfe verfügbar. ■ Die Seite "Unterstützte Produkte von A-Z" ist unter folgender URL verfügbar: http://www.symantec.com/business/support/index?page=products Öffnen Sie die Supportseite Ihres Produkts und klicken Sie dann unter "Allgemeine Themen" auf "Dokumentation".

Dokument	Beschreibung	Speicherort
Hilfe	Informationen zur Verwendung dieses Produkts, einschließlich detaillierter technischer Informationen und Anweisungen zur Ausführung von Routineaufgaben. Hilfe ist für "Solution" und "Suite" verfügbar. Diese Informationen sind im Format "HTML-Hilfe" verfügbar.	Die Dokumentationsbibliothek ist in der "Symantec Management Console" im Menü Hilfe verfügbar. Kontextbezogene Hilfe ist für die meisten Dialogfelder der Symantec Management Console verfügbar. Es gibt folgende Möglichkeiten zum Öffnen der kontextbezogenen Hilfe: ■ Klicken Sie auf die Seite und drücken Sie dann die Taste "F1". ■ Verwenden Sie den Befehl "Kontext", der in der Symantec Management Console im Menü "Hilfe" verfügbar ist.

Zusätzlich zur Produktdokumentation können Sie die folgenden Ressourcen nutzen, um sich mit Symantec-Produkten vertraut zu machen.

Tabelle 1-2 Symantec-Produkt-Informationsressourcen

Ressource	Beschreibung	Speicherort
SymWISE-Support-datenbank	Artikel zu Symantec-Produkten sowie Vorfälle und Probleme im Zusammenhang mit Symantec-Produkten.	http://www.symantec.com/business/theme.jsp?themeid=support-knowledgebase

Ressource	Beschreibung	Speicherort
Symantec Connect	Eine Online-Ressource, die Foren, Artikel, Blogs, Downloads, Ereignisse, Videos, Gruppen und Ideen für Benutzer von Symantec-Produkten enthält.	http://www.symantec.com/connect/endpoint-management/forums/endpoint-management-documentation Hier finden Sie die Liste von Links zu den verschiedenen Gruppen auf Connect: ■ Bereitstellung und Imaging http://www.symantec.com/connect/groups/deployment-and-imaging ■ Erkennung und Inventarisierung http://www.symantec.com/connect/groups/discovery-and-inventory ■ ITMS-Administrator http://www.secure.symantec.com/connect/groups/itms-administrator ■ Mac-Verwaltung http://www.symantec.com/connect/groups/mac-management ■ Monitor Solution und Serverzustand http://www.symantec.com/connect/groups/monitor-solution-and-server-health ■ Patch-Management http://www.symantec.com/connect/groups/patch-management ■ Berichterstellung http://www.symantec.com/connect/groups/reporting ■ ServiceDesk http://www.symantec.com/connect/groups/symantec-servicedesk ■ Software Management http://www.symantec.com/connect/groups/software-management ■ Workflow http://www.symantec.com/connect/ogproduct/symantec-workflow ■ Workspace Virtualization und Streaming http://www.symantec.com/connect/groups/workspace-virtualization-and-streaming

Kapitel 2

Die Komponenten von IT Management Suite

In diesem Kapitel werden folgende Themen behandelt:

- Info zur Symantec Management-Plattform
- Architekturkomponenten von Symantec Management-Plattform
- Komponenten der Symantec Management-Plattform
- Lösungen der IT Management Suite
- Info zu Cloud-fähiger Verwaltung
- Bereitstellen von Software mithilfe von Deployment Solution

Info zur Symantec Management-Plattform

Symantec Management-Plattform bietet Dienste, die von IT-bezogenen Lösungen genutzt werden. Lösungen werden in die Plattform integriert, sodass sie die Dienste der Plattform, wie z. B. Sicherheit, Berichterstattung, Kommunikation, Paketverteilung und Configuration Management Database (CMDB)-Daten nutzen können. Da Lösungen die gleiche Plattform verwenden, können sie sowohl Plattformdienste als auch Daten gemeinsam nutzen. Gemeinsam genutzte Daten sind in der Regel nützlicher als lösungsspezifische. Beispiel: Eine Lösung sammelt Daten über die Software, die auf Unternehmenscomputern installiert ist und eine andere Lösung nutzt die Daten, um Softwarelizenzen zu verwalten. Und eine dritte Lösung kann dieselben Daten zur Softwareaktualisierung verwenden. Diese enge Integration von Lösungen und Plattform erleichtert die Verwendung der verschiedenen Lösungen, da sie alle in einer gemeinsamen Umgebung und über eine gemeinsame Benutzerschnittstelle verwaltet werden.

Die Plattform stellt die folgenden Dienste zur Verfügung:

- Rollenbasierte Sicherheit
- Clientkommunikation und -verwaltung
- Ausführen von geplanten oder von Ereignissen ausgelösten Aufgaben und Richtlinien
- Verteilen und Installieren von Paketen
- Berichterstellung
- Zentralisierte Verwaltung über eine einzelne, gemeinsame Benutzerschnittstelle
- Configuration Management Database (CMDB)
- Software Management Framework

Wenn Sie eine Lösung oder Suite installieren, wird auch die Plattform installiert, wenn dies nicht bereits geschehen ist.

Siehe "Komponenten der Symantec Management-Plattform" auf Seite 23.

Architekturkomponenten von Symantec Management-Plattform

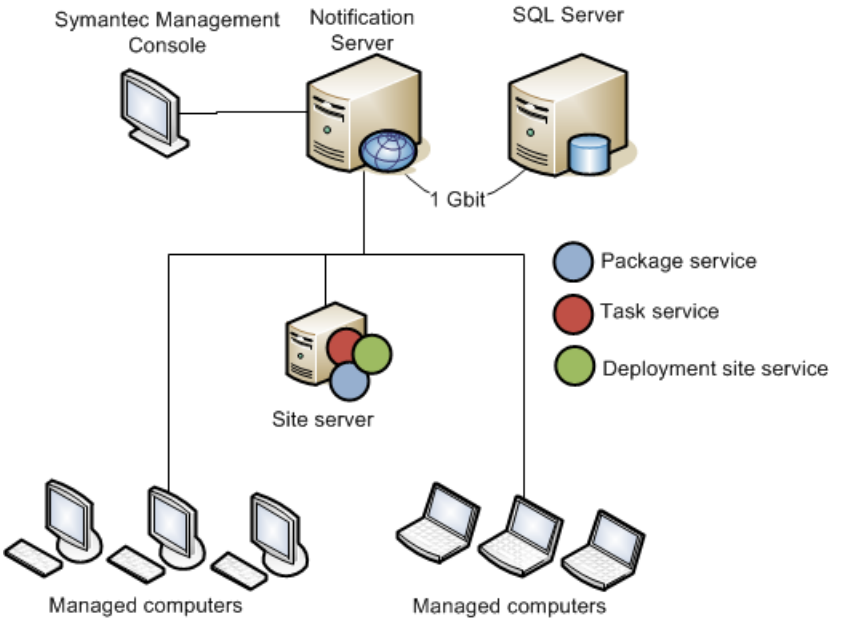
Symantec Management-Plattform enthält vier Hautptarchitekturkomponenten.

Siehe "Überlegungen zu Planung der IT-Verwaltung" auf Seite 37.

Sie lauten:

- Notification Server und seine webbasierte Symantec Management Console
- SQL Server
- Site Server
  Site Server können Task Server, Package Server und Netzwerkstartserver enthalten.
- Verwaltete Computer

Abbildung 2-1 Architekturkomponenten von Symantec Management-Plattform



Komponenten der Symantec Management-Plattform

Tabelle 2-1 Komponenten der Symantec Management-Plattform

Komponente	Beschreibung
Notification Server und Symantec Management Console	Dieser Symantec Management-Plattform-Dienst verarbeitet Ereignisse, stellt die Kommunikation mit verwalteten Computern her und koordiniert die Funktionen der anderen Symantec Management-Plattform-Dienste. Die Konsole ist die webbasierte Benutzeroberfläche des Notification Server-Computers, mit der Sie die Plattform und ihre Lösungen verwalten können.
Configuration Management Database (CMDB)	Die Datenbank, in der alle Informationen über verwaltete Computer gespeichert sind.
Site Server	Symantec Management-Plattform kann einige Typen von Middleware-Komponenten hosten, z. B. Paketdienste, Aufgabedienste und Deployment Site-Dienste. Der offizielle Name für eine Middleware-Komponente ist "Site Service". Komponenten, die als Host für einen Site Service fungieren, werden als "Site Server" bezeichnet. Site Server können eine oder mehrere dieser Dienste hosten.

Komponente	Beschreibung
Symantec Management-Agent	Die Software, die auf einem Computer installiert wird, damit er von Notification Server überwacht und verwaltet werden kann. Nachdem der Symantec Management-Agent installiert ist, ist dieser Computer ein verwalteter Computer.
Software Management Framework	Eine Schnittstelle, mit der Sie Software-Ressourcen aus dem Softwarekatalog erstellen und verwalten können. Außerdem können Sie damit die Pakete in der Softwarebibliothek verwalten. Die Anzeige "Software" stellt einen zentralen Ort zum Initiieren der softwarebezogenen Aufgaben bereit, die in Ihrem Unternehmen durchgeführt werden.
Berichte	Ein Verfahren zum automatisierten Sammeln von Informationen. Sie können Berichte für verwaltete Computer von der Symantec Management Console aus anzeigen.

Siehe "Info zur Symantec Management-Plattform" auf Seite 21.

Lösungen der IT Management Suite

Tabelle 2-2 IT Management Suite -Lösungen und -Komponenten

Suite/Plattform	Lösung/Komponente	Beschreibung
Asset Management Suite	Asset Management Solution	Asset Management Solution ermöglicht das Einrichten und Verwalten verschiedener Asset Management-Prozesse. Sie hilft Ihnen bei der Bewertung Ihrer Assets, der Nachverfolgung von Besitzern und der Beibehaltung von Zuordnungen mit verwandten Dokumenten. Zusätzlich stimmt sie mit ITIL-Standards überein.
	Barcode Solution	Barcode Solution bietet Ihrem Unternehmen eine einfachere und genauere Methode zur Sammlung und Überprüfung von Asset-Informationen. Mit Barcode Solution können Sie die Eingabe von Asset-Daten beschleunigen, Fehler reduzieren, Assets verfolgen und überwachen sowie Inventar verwalten.
	CMDB Solution	In CMDB Solution können Sie Konfigurationselemente, Ressourcen und die Beziehungen zwischen ihnen in einer einzelnen, zentralen Datenbank erstellen. Sie können die Erkennung aller Komponenten und Beziehungen erleichtern und alle erforderlichen Änderungen vornehmen. Die Lösung verwaltet aktiv Ressourcen entsprechend den benutzerspezifischen Anweisungen in Aufträgen, Aufgaben, Konfigurationsrichtlinien und benutzerdefinierten CMDB-Regeln.

Suite/Plattform	Lösung/Komponente	Beschreibung
Client Management Suite	Deployment Solution	Mit Deployment Solution können die Kosten für die Bereitstellung und Verwaltung von Servern, Desktops und Thin Clients von einem zentralen Standpunkt in Ihrer Umgebung aus reduziert werden. Die Lösung bietet Betriebssystembereitstellung, Konfiguration, PC-Persönlichkeitsmigration und Softwarebereitstellung über verschiedene Hardwareplattformen und Betriebssysteme hinweg.
	Inventory Solution	Mit Inventory Solution können Sie Inventardaten zu Computern, Benutzern, Betriebssystemen und installierten Softwareanwendungen in Ihrer Umgebung erfassen. Sie können Inventardaten von Computern erfassen, auf denen Windows, UNIX, Linux und Mac ausgeführt werden. Nachdem Sie Inventardaten gesammelt haben, können Sie diese mithilfe vordefinierter oder benutzerdefinierter Berichte analysieren.
	IT Analytics	Die IT Analytics Solution-Software ergänzt und erweitert die traditionelle Berichterstellung, die in den meisten Altiris-Lösungen angeboten wird. Sie erweitert den Notification Server um neue Funktionen zur mehrdimensionalen Analyse und robusten grafischen Berichterstellung und Verteilung. Diese Funktionalität ermöglicht es Benutzern, Daten selbst zu untersuchen, ohne die Datenbanken oder die Berichterstellungstools von anderen Herstellern genau kennen zu müssen. Sie ermöglicht es Benutzern, ihre eigenen Fragen schnell, leicht und effektiv zu stellen und zu beantworten.

Suite/Plattform	Lösung/Komponente	Beschreibung
	Patch Management Solution	Mit Patch Management Solution für Windows können Sie Windows-Computer auf erforderliche Updates scannen und die Ergebnisse des Scans werden angezeigt. Mit dem System den Download und die Verteilung von Softwareupdates automatisieren. Sie können Filter der Computer erstellen und den Patch auf die Computer anwenden, die ihn benötigen. Patch Management Solution für Linux dient dazu, Red Hat- und Novell Linux-Computer auf Sicherheitslücken zu scannen. Die Ergebnisse werden anschließend angezeigt. Die Vorgänge zum Herunterladen und Verteilen der Softwareupdates können automatisiert werden. Die Lösung lädt die erforderlichen Patches herunter und stellt Assistenten zur Verfügung, um Ihnen zu helfen, sie zu implementieren. Mit Patch Management Solution für Mac können Sie Mac-Computer auf erforderliche Updates hin prüfen. Die Ergebnisse werden anschließend angezeigt. Die Vorgänge zum Herunterladen und Verteilen der erforderlichen Updates können automatisiert werden. Sie können alle oder nur einige der Updates verteilen.
	pcAnywhere Solution	pcAnywhere Solution ist eine Fernsteuerungslösung. Mit ihrer Hilfe können Sie Computer verwalten, Helpdesk-Probleme lösen und Verbindungen zu standortfernen Geräten herstellen.
	Real-Time System Manager	Real-Time System Manager liefert Ihnen ausführliche Echtzeitinformationen über einen verwalteten Computer und ermöglicht es Ihnen, über Fernzugriff verschiedene administrative Aufgaben in Echtzeit durchzuführen. Mit Real-Time System Manager können Sie auch einige der Verwaltungsaufgaben auf eine Computergruppe anwenden. Sie können die Aufgaben sofort oder nach einem Zeitplan ausführen.

Suite/Plattform	Lösung/Komponente	Beschreibung
	Software Management Solution	Software Management Solution stellt intelligente und bandbreitensensible Verteilung und Verwaltung von Software über eine zentrale Internet-Konsole zur Verfügung. Es nutzt den Softwarekatalog und die Softwarebibliothek, um sicherzustellen, dass die erforderliche Software installiert wird, installiert bleibt und ohne Störung durch andere Software läuft. Software Management Solution unterstützt Softwarevirtualisierungstechnologie, mit der Sie Software in eine virtuelle Schicht auf dem Clientcomputer installieren können. Außerdem können Benutzer mit Software Management Solution direkt genehmigte Software herunterladen und installieren oder andere Software anfragen.
	Symantec Endpoint Protection- Integrations-komponente	Die Symantec Endpoint Protection-Integrationskomponente kombiniert Symantec Endpoint Protection mit Ihren anderen Symantec Management-Plattform-Lösungen. Sie können Computer inventarisieren, Patches aktualisieren und Software sowie neue Computer verteilen. Sie können auch Ihre Systeme und Daten sichern und wiederherstellen und DLP-Agents sowie Symantec Endpoint Protection-Clients verwalten. Sie können diese Aufgaben von einer einzelnen, webbasierten Symantec Management Console aus erledigen.
	Workflow Solution	Symantec Workflow ist ein Sicherheitsprozessentwicklungs-Framework, das Sie nutzen können, um automatisierte Geschäfts- und Sicherheitsprozesse zu erstellen. Diese Prozesse sorgen für erhöhte Wiederholbarkeit, Kontrolle und Verantwortlichkeit bei gleichzeitiger Reduzierung der Gesamtarbeitslast. Mit dem Symantec Workflow-Framework können Sie auch Workflow-Prozesse erstellen, die Symantec-Tools in die eindeutigen Geschäftsprozesse Ihrer Organisation integrieren. Nach der Bereitstellung können Workflow-Prozesse auf Umgebungsvariablen automatisch reagieren. Workflow-Prozesse können auch Benutzerschnittstellenpunkte ermöglichen, wenn der Prozess jemanden erfordert, der eine Entscheidung mit Verantwortlichkeit treffen soll.
Server Management Suite	Deployment Solution	Mit Deployment Solution können die Kosten für die Bereitstellung und Verwaltung von Servern, Desktops und Thin Clients von einem zentralen Standpunkt in Ihrer Umgebung aus reduziert werden. Die Lösung bietet Betriebssystembereitstellung, Konfiguration, PC-Persönlichkeitsmigration und Softwarebereitstellung über verschiedene Hardwareplattformen und Betriebssysteme hinweg.

Suite/Plattform	Lösung/Komponente	Beschreibung
	Inventory Solution	Mit Inventory Solution können Sie Inventardaten zu Computern, Benutzern, Betriebssystemen und installierten Softwareanwendungen in Ihrer Umgebung erfassen. Sie können Inventardaten von Computern erfassen, auf denen Windows, UNIX, Linux und Mac ausgeführt werden. Nachdem Sie Inventardaten gesammelt haben, können Sie diese mithilfe vordefinierter oder benutzerdefinierter Berichte analysieren.
	Inventory Pack für Server	Inventory Pack for Servers erfasst serverbasierte Inventardaten von Servern. Es wird in Inventory Solution ausgeführt und verwendet die gleichen Inventory-Plugins, -Aufgaben und -Assistenten.
	IT Analytics	Die IT Analytics Solution-Software ergänzt und erweitert die traditionelle Berichterstellung, die in den meisten Altiris-Lösungen angeboten wird. Sie erweitert den Notification Server um neue Funktionen zur mehrdimensionalen Analyse und robusten grafischen Berichterstellung und Verteilung. Diese Funktionalität ermöglicht es Benutzern, Daten selbst zu untersuchen, ohne die Datenbanken oder die Berichterstellungstools von anderen Herstellern genau kennen zu müssen. Sie ermöglichen es Benutzern, ihre eigenen Fragen schnell, leicht und effektiv zu stellen und zu beantworten. Das Altiris IT Analytics Symantec Endpoint Protection-Paket ist ebenfalls in dieser Lösung enthalten.
	Monitor Solution	Mit Monitor Solution für Server können Sie verschiedene Aspekte der Betriebssysteme, Anwendungen und Geräte überwachen. Diese Aspekte können Ereignisse, Prozesse und die Leistung beinhalten. So können Sie sicherstellen, dass Server und Geräte funktionieren und die Kosten für die Server- und Netzwerküberwachung reduzieren.
	Monitor Pack für Server	Monitor Pack für Server funktioniert mit den Monitor Solution-Kernkomponenten der Symantec Management-Plattform. Mit ihr können Sie die Betriebssystemleistung, Dienste und Ereignisse Ihrer Windows-, UNIX- und Linux-Serverumgebung überwachen.

Suite/Plattform	Lösung/Komponente	Beschreibung
	Patch Management Solution	Mit Patch Management Solution für Windows können Sie Windows-Computer auf erforderliche Updates scannen und die Ergebnisse des Scans werden angezeigt. Mit dem System den Download und die Verteilung von Softwareupdates automatisieren. Sie können Filter der Computer erstellen und den Patch auf die Computer anwenden, die ihn benötigen. Patch Management Solution für Linux dient dazu, Red Hat- und Novell Linux-Computer auf Sicherheitslücken zu scannen. Die Ergebnisse werden anschließend angezeigt. Die Vorgänge zum Herunterladen und Verteilen der Softwareupdates können automatisiert werden. Die Lösung lädt die erforderlichen Patches herunter und stellt Assistenten zur Verfügung, um Ihnen zu helfen, sie zu implementieren. Mit Patch Management Solution für Mac können Sie Mac-Computer auf erforderliche Updates hin prüfen. Die Ergebnisse werden anschließend angezeigt. Die Vorgänge zum Herunterladen und Verteilen der erforderlichen Updates können automatisiert werden. Sie können alle oder nur einige der Updates verteilen.
	Real-Time System Manager	Real-Time System Manager liefert Ihnen ausführliche Echtzeitinformationen über einen verwalteten Computer und ermöglicht es Ihnen, über Fernzugriff verschiedene administrative Aufgaben in Echtzeit durchzuführen. Mit Real-Time System Manager können Sie auch einige der Verwaltungsaufgaben auf eine Computergruppe anwenden. Sie können die Aufgaben sofort oder nach einem Zeitplan ausführen.
	Software Management Solution	Software Management Solution stellt intelligente und bandbreitensensible Verteilung und Verwaltung von Software über eine zentrale Internet-Konsole zur Verfügung. Es nutzt den Softwarekatalog und die Softwarebibliothek, um sicherzustellen, dass die erforderliche Software installiert wird, installiert bleibt und ohne Störung durch andere Software läuft. Software Management Solution unterstützt Softwarevirtualisierungstechnologie, mit der Sie Software in eine virtuelle Schicht auf dem Clientcomputer installieren können. Außerdem können Benutzer mit Software Management Solution direkt genehmigte Software herunterladen und installieren oder andere Software anfragen.

Suite/Plattform	Lösung/Komponente	Beschreibung
	Symantec Endpoint Protection-Integrationskomponente	Die Symantec Endpoint Protection-Integrationskomponente kombiniert Symantec Endpoint Protection mit Ihren anderen Symantec Management-Plattform-Lösungen. Sie können Computer inventarisieren, Patches aktualisieren und Software sowie neue Computer verteilen. Sie können auch Ihre Systeme und Daten sichern und wiederherstellen und DLP-Agents sowie Symantec Endpoint Protection-Clients verwalten. Sie können diese Aufgaben von einer einzelnen, webbasierten Symantec Management Console aus erledigen.
	Virtual Machine Management	Virtual Machine Management ist eine Komponente von Server Management Suite, mit dem Sie den Virtualisierungprozess auf Ihrem Netzwerk durchführen können. Sie können virtuelle Umgebungen mit Servern, Speichergeräten und Netzwerkressourcen auf einem einzelnen physischen Computer erstellen. Virtualisierung erhöht die Leistungsfähigkeit und die Produktivität von Hardwareressourcen und hilft, administrative Kosten zu reduzieren.
	Workflow Solution	Symantec Workflow ist ein Sicherheitsprozessentwicklungs-Framework, das Sie nutzen können, um automatisierte Geschäfts- und Sicherheitsprozesse zu erstellen. Diese Prozesse sorgen für erhöhte Wiederholbarkeit, Kontrolle und Verantwortlichkeit bei gleichzeitiger Reduzierung der Gesamtarbeitslast. Mit dem Symantec Workflow-Framework können Sie auch Workflow-Prozesse erstellen, die Symantec-Tools in die eindeutigen Geschäftsprozesse Ihrer Organisation integrieren. Nach der Bereitstellung können Workflow-Prozesse auf Umgebungsvariablen automatisch reagieren. Workflow-Prozesse können auch Benutzerschnittstellenpunkte ermöglichen, wenn der Prozess jemanden erfordert, der eine Entscheidung mit Verantwortlichkeit treffen soll.

Siehe "Informationen zur IT Management Suite" auf Seite 11.

Die Anwendung "ITMS Admin Mobile" ist eine mobile iPad-Anwendung, mit der Sie einige ITMS-Aufgaben unterwegs ausführen können. Zu den Funktionen zählt die Fähigkeit, die Patch Management- und Software Delivery-Compliance-Berichte anzuzeigen sowie Aktionen auf Geräten durchzuführen. Funktionen für ITMS Admin sind bereits serverseitig in ITMS 7.5 enthalten. Sie müssen also nur noch die Anwendung auf Ihr Gerät herunterladen und sich mit Ihren Domänenanmeldeinformationen auf Ihrem Gerät anmelden.

Info zu Cloud-fähiger Verwaltung

Mit der Cloud-fähigen Verwaltung können Sie Endgeräte über das Internet verwalten, selbst, wenn sich die Clientcomputer außerhalb der Unternehmensumgebung befinden und nicht direkt auf die Management-Server zugreifen können. Die verwalteten Computer benötigen keine VPN-Verbindung zu Ihrem Unternehmensnetzwerk.

Sie können die Cloud-fähige Verwaltung in folgenden Szenarien anwenden:

- In Unternehmen, in denen viele Mitarbeiter reisen oder außerhalb des Büros arbeiten (außerhalb des Intranets des Unternehmens).
- Ein MSP (Managed Service Provider), der externe Unternehmen verwaltet.
- Bei hoch verteilten Unternehmen mit vielen kleinen Büros oder Angestellten, die von zu Hause aus arbeiten.

Wenn Sie die Cloud-fähige Verwaltung implementieren, besteht keine direkte Verbindung zwischen Notification Server-Computer, Site Server und dem Internet. Deshalb kommuniziert Symantec Management Agent mit dem Notification Server-Computer und den Site Servern über ein Internet-Gateway. Normalerweise sollten zwei oder mehr Internet-Gateways verfügbar sein, um eine zuverlässige Verwaltung von Cloud-fähigen Clients beizubehalten und Failoveroptionen zur Verfügung zu stellen. Jedes Gateway kann das Weiterleiten an mehrere unabhängige Notification Server unterstützen.

Zur Verwendung der Cloud-fähigen Verwaltung müssen Sie einen Internet-Gatewayserver installieren. Das Internet-Gateway fungiert als Tunnelling-Proxy. Es stellt den Datenschutz und die Sicherheit der Daten sicher, die zwischen einen Agent und einen Management-Server mit HTTPS-Kommunikationen geleitet geworden wird. Das Internet-Gateway befindet sich in einer demilitarisierten Zone (DMZ) zwischen zwei Firewalls. Es akzeptiert eingehende Verbindungen von autorisierten Clientcomputern im Internet und leitet sie an die entsprechenden Notification Server und Site Server innerhalb Ihres Netzwerks weiter. Das Gateway blockiert alle Verbindungsversuche durch nicht autorisierte Clients.

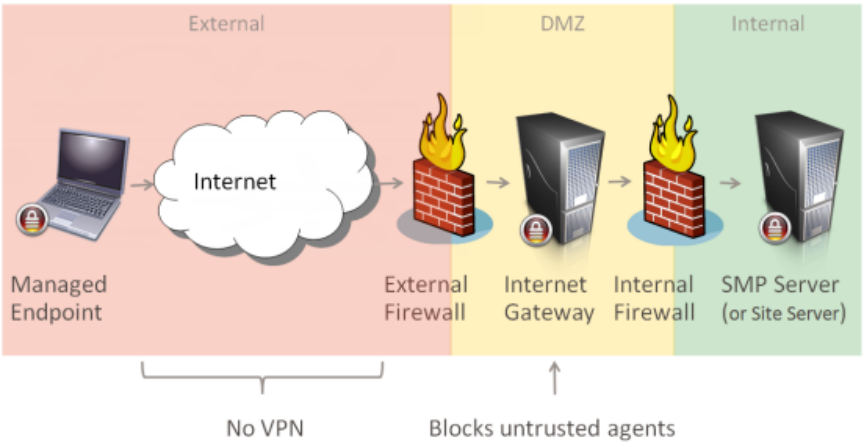
Symantec Management Agent legt automatisch fest, ob es erforderlich ist, die Kommunikation über das Internet-Gateway umzuleiten oder nicht. Wenn ein Cloud-fähiger Computer über das VPN Direktzugriff zum lokalen Netzwerk hat, wechselt der Agent automatisch zu einer direkten Verbindung mit dem Notification Server. Wenn sich ein Cloud-fähiger Computer außerhalb des Unternehmensnetzwerks befindet, leitet der Agent alle Internetverbindungen über das Internet-Gateway auf den Notification Server um.

Siehe "Empfohlene Internet-Gateway-Hardware" auf Seite 66.

Hinweis: Die Cloud-fähige Verwaltung wird nur auf Microsoft Windows-Clientcomputern unterstützt.

Die Cloud-fähige Verwaltung ist nur dann auf Ihrer Symantec Management-Plattform verfügbar, wenn eine oder mehrere der installierten Lösungen Cloud-fähige Verwaltung unterstützen. Nicht alle Symantec-Lösungen unterstützen die Cloud-fähige Verwaltung in der IT Management Suite 7.5. Weitere Informationen zur Unterstützung der Cloud-fähigen Verwaltung für eine bestimmte Lösung finden Sie in der Dokumentation der jeweiligen Lösung.

Abbildung 2-2 Cloud-fähige Verwaltung



Um die Cloud-fähige Verwaltung nutzen zu können, müssen Sie die folgenden Aufgaben durchführen:

- Richten Sie die Infrastruktur ein und konfigurieren Sie Ihre Server und Clientcomputer so, dass sie SSL verwenden.
- Installieren und konfigurieren Sie die Internet-Gateways, konfigurieren Sie die Richtlinien für die Cloud-fähige Verwaltung und richten Sie die Symantec Management Agents so ein, dass sie die Umgebung der Cloud-fähigen Verwaltung unterstützen.
- (Optional) Führen Sie Fehlerbehebungs- und Wartungsaufgaben durch.

Bereitstellen von Software mithilfe von Deployment Solution

Mit Deployment Solution können Sie Hardware-unabhängige Images erstellen und bereitstellen, Betriebssysteme installieren und sie für Clientcomputer wie Desktopcomputer, Server und Notebooks von einer zentralen Stelle aus verwalten. Die Lösung ermöglicht es auch, Profile zu erfassen und zu verteilen, Systemkonfigurationen zur Laufzeit durchzuführen und Dateien oder Ordner von einem Computer auf einen anderen zu kopieren. Die Anwendung der Deployment Solution hängt vom Typ des Clientcomputers ab, den die Lösung verwaltet. Der Clientcomputer kann ein Bare Metal-Computer, ein vordefinierter Computer oder ein verwalteter Computer sein. Das Rollout der meisten zur Bereitstellung gehörenden Funktionen erfolgt als Aufgaben, die auf den Clientcomputern ausgeführt werden. Deployment Solution ist eng an die Symantec Management-Plattform gekoppelt und nutzt die Funktion der Site Server-Komponenten von SMP, wie etwa Package Server (PS) und Task Server (TS). Die Lösung erfordert, dass PS- und TS-spezifische Bereitstellungskomponenten auf den Site Servern zur Ausführung von Deployment-Aufgaben bereitgestellt werden. Außerdem erfordert Deployment Solution zum Ausführen von Deployment-Aufgaben auf den Clientcomputern, dass auf diesen Computern betriebssystemspezifische Deployment-Plugins installiert sind.

Folgende Deployment Solution-Komponenten sind zum Ausführen von Deployment-Aufgaben erforderlich:

- Deployment Solution Package Server-Komponente
- Deployment Solution Task Server-Komponente
- Deployment Solution-Plugin für die folgenden Betriebssysteme:
  - Windows
  - Linux
  - Mac

Einrichten der Preboot-Umgebung in Deployment Solution

Vor dem Starten der Ausführung von Deployment-Aufgaben müssen Sie in Deployment Solution die Preboot-Konfigurationen erstellen und einrichten. Die erstellten Preboot-Konfigurationen müssen die Clientcomputer starten, um die Deployment-Aufgaben auf ihnen auszuführen. In Deployment Solution gibt es zwei Typen von Preboot-Umgebungen, der Sie entsprechend der folgenden Details konfigurieren können:

Tabelle 2-3

Typ der Preboot-Konfiguration	Beschreibung
Pre-Boot Execution Environment (PXE)	In Deployment Solution wird eine Pre-Boot Execution Environment (PXE) unter Verwendung der "Preboot-Konfiguration" erstellt und über den Network Boot Service (NBS) verteilt, der auf einem Site Server installiert ist. Die NBS-Komponente setzt sich aus dem PXE-Dienst, SymantecNetworkBootService(PXE und BSDP) und dem TFTP-Dienst, SymantecNetworkBootServiceTftp, zusammen. Nachdem ein Computer zu einem Netzwerk hinzugefügt wurde, startet der PXE-Dienst den Computer in der Preboot-Umgebung unter Verwendung eines Preboot-Pakets des unterstützten Betriebssystems. Das Preboot-Paket wird auch als PXE-Image bezeichnet. In Deployment Solution können Sie das Preboot-Paket konfigurieren und die Preboot-Umgebung neu erstellen, bevor Sie das Rollout der konfigurierten Preboot-Umgebung auf den NBS-Site Servern durchführen. Ein konfiguriertes Preboot-Paket enthält die betriebssystemspezifischen PXE-Umgebungsdateien, den betriebssystemspezifischen Agent und das Deployment-Plugin, das auch als Deployment Agent bezeichnet wird. Es können folgende betriebssystemspezifische Preboot-Pakete konfiguriert werden: ■ WinPE für Windows ■ LinuxPE für Linux ■ Netboot für Mac

Typ der Preboot-Konfiguration	Beschreibung
Automationsumgebung	Eine Automationsumgebung ist die konfigurierte Preboot-Umgebung, die lokal auf dem Clientcomputer installiert ist. Eine Automationsumgebungsinstallation ermöglicht es Ihnen, Clientcomputer in der Preboot-Umgebung zu starten. Ähnlich wie die PXE-Umgebung, enthält die Automationsumgebung auch ein betriebssystemspezifisches Preboot-Paket, das auf den Clientcomputern installiert ist. Das als Ordner auf den Clientcomputern installierte Preboot-Paket wird auch als Automatisierungsordner bezeichnet. Standardmäßig lautet der Automatisierungsordner bei Windows-Computern "PEInstall" und bei Linux-Computern wird der Automatisierungsordner "LinInstall" auf dem Clientcomputer erstellt.

Weitere Details über die PXE-Umgebung und die Automationsumgebung finden Sie im *Symantec™ Deployment Solution 7.5 powered by Altiris™ – Benutzerhandbuch*.

Methoden zur Verteilung von Preboot-Umgebungen

Clientcomputer starten in der Preboot-Umgebung über den Network Boot Service (NBS), der auf dem Site Server installiert ist. NBS muss entsprechend des Typs des zu startenden Clientcomputers konfiguriert werden. Die Typen von Clientcomputern, die Deployment Solution starten und verwalten, sind unbekannte Computer, vordefinierte Computer und verwaltete Computer. Die Konfiguration von NBS kann über die Symantec Management Console durchgeführt werden.

Weitere Details zum Konfigurieren von Typen von Clientcomputern über NBS finden Sie im *Symantec™ Deployment Solution 7.5 powered by Altiris™ – Benutzerhandbuch*

Hauptmerkmale von Deployment Solution

Die zwei Hauptmerkmale von Deployment Solution sind folgende:

- Imaging-Funktionen von Deployment Solution
  Mit Deployment Solution können Sie ein Image eines Clientcomputers erstellen und auf mehreren Clientcomputern bereitstellen. Wenn ein Image erstellt wird, wird ebenfalls eine Symantec Management-Plattform-Ressource für dieses

Image erstellt. Die Ressource wird als ein Paket auf Notification Server gespeichert und an Package Server verteilt, die im Netzwerk vorhanden sind. Die Image-Ressource wird beim Erstellen von Aufgaben zum Bereitstellen von Images verwendet. Wenn eine Image-Bereitstellungsaufgabe an einen Clientcomputer gesendet wird, ruft er das Image von dem Package Server ab, der dem Clientcomputer am nähesten ist.

Sie können Datenträger-Images und Backup-Images von Clientcomputern erstellen. Deployment Solution liefert das Ghost- und das RapiDeploy-Tool zum Erstellen von Images von Clientcomputern, auf denen ein Windows- oder Linux-Betriebssystem installiert ist, und das symDeploMac-Tool zum Erstellen von Images für Clientcomputer, auf denen ein Mac-Betriebssystem installiert ist.

Weitere Details zum Erstellen und Bereitstellen von Images finden Sie im *Symantec™ Deployment Solution 7.5 powered by Altiris™ – Benutzerhandbuch*.

- Installieren der Betriebssystemfunktionen von Deployment Solution

  Mit Deployment Solution können Sie Windows-, Linux- und Mac-Betriebssysteme auf Clientcomputern installieren. Um ein Betriebssystem auf dem Clientcomputer zu installieren, müssen Sie den Clientcomputer zunächst in der Preboot-Umgebung des Betriebssystems starten, das Sie auf dem Clientcomputer installieren möchten. Deployment Solution stellt betriebssystemspezifische Aufgaben zum Installieren des Betriebssystems auf den Clientcomputern bereit.

  Für Windows und Mac werden die Pakete der Betriebssysteme auf Notification Server hinzugefügt und von dort an alle Package Servern im Netzwerk verteilt. Wenn eine Aufgabe zur Installation eines Betriebssystems an einen Clientcomputer gesendet wird, ruft er das Paket von dem Package Server ab, der dem Clientcomputer am nähesten ist. Für Linux werden die Betriebssystempakete auf einem anonymen HTTP- oder FTP-Server abgelegt.

  Weitere Details zum Installieren von Betriebssystemen finden Sie im *Symantec™ Deployment Solution 7.5 powered by Altiris™ – Benutzerhandbuch*.

Kapitel 3

Planung für IT Management Suite

In diesem Kapitel werden folgende Themen behandelt:

- Überlegungen zu Planung der IT-Verwaltung
- Informationen zur Planung Ihrer SQL Server-Konfiguration
- Informationen zur Planung Ihrer Site Server
- Symantec Management Agent-Bereitstellungsplanung
- Info zu Agent-Registrierung

Überlegungen zu Planung der IT-Verwaltung

Viele Faktoren und Überlegungen können einen Umsetzungsplan beeinflussen. Um Ihre Symantec Management-Plattform-Infrastruktur zu entwickeln, müssen Sie Ihre speziellen organisatorischen Funktionen und Anforderungen einschätzen.

Siehe "Architekturkomponenten von Symantec Management-Plattform" auf Seite 22.

Ihre Anforderungen können einige Variablen umfassen. Einige diese Variablen können Folgendes beinhalten:

- Die geografischen Auswirkungen der Umgebung.
  Beim Entwurf einer zentralen Verwaltung werden mehrere Notification Server-Computer verwendet, um eine Vielzahl von IT-Verteilungsmodellen zu unterstützen. Beispielsweise können eine Unternehmenszentrale mit Tausenden von verwalteten Computern sowie große Niederlassungen und kleine Niederlassungen vorhanden sein. Der zentrale Entwurf kann zum Verwalten von globalen Richtlinien und Aufgaben geeignet sein. Wenn Ihre IT-Organisation primär einen zentralisierten Aufbau hat, dann kann die Symantec

Management-Plattform entsprechend entwickelt werden, um sie zu unterstützen. In einer solchen Umgebung verwendet die Plattform möglicherweise einen übergeordneten Notification Server-Computer, der mit weiteren untergeordneten Notification Server-Computern verbunden ist.

Ein dezentralisierter Verwaltungsentwurf besteht aus mehreren verstreuten Standorten und Netzwerksegmenten, die untergeordnete Standorte und Netzwerksegmente unterstützen. Bei einem dezentralisierten Entwurf wird keine Hierarchie verwendet, sondern es werden stattdessen mehrere Notification Server-Computer, die voneinander unabhängig arbeiten, verwendet.

- Das zukünftige Wachstum der Organisation.

  Der Infrastrukturentwurf erfordert möglicherweise Raum für Wachstum. Wenn möglich, sollte die Architektur die aktuelle Organisation und die Vision für die Organisation in den kommenden Jahren darstellen.

- Die Verteilung und die Richtlinien des IT-Verwaltungsteams.'

  Die Vorgänge, die von IT zentral und lokal verwaltet werden, beeinflussen den Entwurf. Einige IT-Aufgaben müssen möglicherweise von einem zentralen Standort aus ausgeführt werden, andere Aufgaben dagegen von lokalen Standorten. Die Sicherheitsrichtlinien der Organisation beeinflussen den Entwurf.

  Ihre Organisationsstruktur legt möglicherweise die Platzierung der Komponenten und den Entwurf der Infrastruktur fest. Der tägliche Arbeitsablauf des Personals der Organisation und der Aufbau des Geschäftsprozesses beeinflussen den Plan. Verschiedene Niederlassungen der Organisation, Sicherheitsanforderungen oder geographischen Anforderungen erfordern möglicherweise separate Notification Server-Verwaltungsdomänen. Verschiedene Gruppen und die Rollen, die Endgeräte verwalten, erfordern möglicherweise rollen- und bereichsbasierte Sicherheit für den Notification Server. Rollen- und bereichsbasierte Sicherheit bedeutet zusätzliche Arbeitslast für den Notification Server-Computer.

- Die Konnektivitätsbereiche der Umgebung.

  Die Konnektivitätsbereiche der Umgebung legen möglicherweise die Platzierung von Komponenten fest. Angenommen, es gibt einen Standort der ersten Ebene, die gut vernetzt ist, aber die Standorte der zweiten Ebenen verfügen über unzulängliche Verbindungen. Benutzer, die auf Geschäftsreisen sind, können Wählverbindungen oder ein VPN von einem Remote-Standort.

- Die installierten Lösungen und wie intensiv sie genutzt werden.

  Die Anzahl von installierten und intensiv genutzten Lösungen beeinflusst die Anzahl von verwalteten Computern, die ein Notification Server unterstützen kann. Beispielsweise kann ein Server, auf dem nur Inventory Solution installiert ist, mehr Endgeräte bedienen als ein Server, auf dem die gesamte IT Management Suite installiert ist.

- Die Notwendigkeit der parallelen Konsolennutzung und Berichterstellung.

Die parallele Nutzung der Symantec Management Console kann den Prozessor zusätzlich belasten. Sie können die Konsole verwenden, um benutzerdefinierte Berichte zu erstellen und Informationen über die Umgebung anzuzeigen. Viele benutzerdefinierten Berichte werden mit erweiterten SQL-Anweisungen geschrieben, die eine beträchtliche Rechenleistung der Datenbank erfordern. Wenn viele Benutzer diese Berichte gleichzeitig auf dem Notification Server-Computer ausführen, kann seine Leistung dadurch beeinträchtigt werden.

Wenn die Organisation eine intensive benutzerdefinierte Berichterstellung erfordert, erwägen Sie, einen separaten Notification Server für die Berichterstellung zu implementieren. Dies bedeutet zwar, dass die Organisation in einen weiteren Server investieren muss, sie erhält dafür jedoch eine Infrastruktur mit Aufgabentrennung. Der Notification Server-Computer, der für das Verwalten von Endgeräten verantwortlich ist, kann seine Rechenleistung dieser Funktion widmen. Der Notification Server-Computer, der für die Bereitstellung von Berichten verantwortlich ist, setzt seine Rechenleistung für diese andere Funktion ein. Bei dieser Konfiguration können mithilfe von Standalone-Replikation Ressourceninventarisierungsinformationen von dem Notification Server-Computer, der für die Agents zuständig ist, an den für die Berichterstellung zuständigen Notification Server-Computer weitergeleitet werden.

Außerdem sind die Arbeitsspeicherkosten zu berücksichtigen, die mit jeder gleichzeitigen Konsolensitzungen vom IIS auf dem Notification Server-Computer verbunden sind. Zur Berechnung dieser Arbeitsspeicheranforderung können Sie ungefähr 20 MB pro Konsolenverbindung ansetzen.

Informationen zur Planung Ihrer SQL Server-Konfiguration

Die folgenden Informationen geben Richtlinien für SQL-Server-Konfigurationen für einen Symantec Configuration Management Database(CMDB)-Computer. Sie können diese Richtlinien befolgen, um die Leistung des SQL Server-Computers zu optimieren, der die (CMDB) hostet. Diese Richtlinien sind nicht exklusiv, und zusätzliche Konfigurationsoptionen können je nach den Besonderheiten Ihrer Umgebung angebracht sein. Ausführliche Informationen über die SQL Server-Konfiguration finden Sie in der Microsoft-Dokumentation.

Viele zusätzliche Artikel über die SQL-Server-Installation, -Konfiguration und -Wartung stehen in der SymWISE Support Knowledgebase zur Verfügung. Die SymWISE Support Knowledgebase ist unter www.symantec.com/business/theme.jsp?themeid=support-knowledgebase verfügbar.

Zusätzliche Ressourcen finden Sie im Artikel unter http://www.symantec.com/docs/HOWTO8201 in der SymWISE Support Knowledgebase.

Tabelle 3-1 Zu berücksichtigende Aspekte bei der Planung Ihrer SQL Server-Konfiguration

Aspekt	Beschreibung
Hardware	Sie können empfohlene Hardware-Richtlinien verwenden, um die Leistung Ihres SQL Server-Computers zu optimieren. Siehe Tabelle 4-1 auf Seite 63.
Festplattenkonfiguration	Die Art und Weise, wie Sie die Festplatten Ihres SQL Server-Computers konfigurieren, wirkt sich auf Ihre Gesamtleistung aus. Sie können Datenträgerkonfigurationsempfehlungen verwenden, um den Durchsatz zu maximieren und die Leistung Ihres SQL Server-Computers zu optimieren. Siehe "Info zur Festplattenkonfiguration für SQL Server" auf Seite 41.
Datenbankgröße festlegen	Sie können Richtlinien zur Größenfestlegung von Datenbanken verwenden, um die Leistung Ihres SQL Server-Computers zu optimieren. Siehe "Informationen über die Festlegung der Datenbankgröße für SQL Server" auf Seite 42.
Arbeitsspeicherverwaltung	Sie können Arbeitsspeicherverwaltungs-Richtlinien verwenden, um die Leistung Ihres SQL Server-Computers zu optimieren. Siehe "Info zur Arbeitsspeicherverwaltung für SQL Server" auf Seite 43.
SQL-Wartungsplan	Sie können Wartungsplanempfehlungen verwenden, um die Leistung Ihres SQL Server-Computers zu optimieren. Siehe "Informationen zur Verwaltung der SQL-Datenbank" auf Seite 45.
SQL-Failoverclustering	Sie können SQL-Failoverclustering verwenden. Dies ist eine Methode zum Erstellen einer hohen Verfügbarkeit für Ihre Symantec Management-Plattform. Siehe "Verwenden des Microsoft SQL-Failover-Clustering mit ITMS 7.1 SP2 oder höher" auf Seite 46.

Info zur Festplattenkonfiguration für SQL Server

Der Durchsatz des SQL Servers ist ein primärer Aspekt für die Symantec Management-Plattformleistung. Die Methode, mit der Sie Ihre Festplatten auf SQL Server konfigurieren, beeinflusst den Durchsatz. Wenn Sie Spindellaufwerk (HDD) oder ein Storage Area Network (SAN) verwenden, erwägen Sie, ein ausführliche Durchsatzanalyse durchzuführen, wenn Sie Ihre Entscheidung zwischen einem Festkörperlaufwerk (SSD) und anderen Speicheroptionen treffen. Händler von Speichermedien präsentieren immer wieder neue leistungsstarke Speicher wie SSDs, PCIe Flash und viele andere innovative Wege zur Konfiguration von HDD- oder Hybrid-Laufwerken.

SSD und SAN mit hoher Leistung sind für SQL-Leistung optimal. Es kann wegen hoher IO-Bandbreite und niedrigerer IO-Latenz mehr als eine Million IOPS unterstützen. Vergleichen Sie diese Leistung mit einzelnen HDDs, die nur 150 – 200 IOPS unterstützen. Wenn man HDD verwendet, werden Hochleistung RAID-Konfigurationen mit mehreren Kanälen empfohlen.

Wenn Sie traditionelles HDD in den RAID-Konfigurationen verwenden, gelten RAID 10 und RAID 0+1 als Hochleistung. RAID 5 ist keine Hochleistungkonfiguration und wird nicht empfohlen.

Stellen Sie für eine optimale Leistung sicher, dass das Betriebssystem, die SQL-Datendatei, die TempDB-Datenbank und die Protokolldatei jeweils über einen dedizierten Datenträger verfügen. Um die Leistung weiter zu verbessern, können Sie die Datendatei und die TempDB-Datenbank über mehrere Datenträger splitten. Die Anzahl von Datenträgern, die Sie verwenden, sollte der Anzahl von Prozessorkernen in Ihrem SQL Server entsprechen. Eine Empfehlung für Hochleistung ist, Parallanordnungen mit der gleichen Anzahl von Datenträgern wie Prozessorkernen zu verwenden. Sie können die SQL-Datendatei und die Transaktionsprotokolldatei splitten, damit sie der Anzahl von Prozessorkernen entsprechen.

Die Datendatei setzt sowohl eine hohe Lese-als auch Schreibleistung und Redundanz voraus.

Die TempDB-Datenbank benötigt eine hohe Lese-Schreibleistung, Redundanz ist jedoch nicht notwendig. Die TempDB-Datenbank fungiert als ein vorübergehender Arbeitsbereich für viele Prozesse. Die TempDB-Datenbank setzt Hochgeschwindigkeit voraus; jedoch wird sie nicht für Speicher verwendet und wird regelmäßig bereinigt.

Das Transaktionsprotokoll erfordert auch einen hohen Datenträgerdurchsatz für optimale Systemleistung.

On-Box-Konfiguration

Eine kombinierte Notification Server- und SQL-Datenbankinstallation kann auf HDD, einem Festkörperlaufwerk oder einer Kombination aus beidem installiert werden. Wir empfehlen, dass Sie gespiegelte HDD für das Betriebssystem und den Notification Server verwenden, und SSD für die SQL-Datenbank. Dieser Ansatz liefert die beste Kombination aus Leistung, Kosteneffizienz und einfacher Implementierung. Wenn Sie SAN-Speicher für SQL verwenden, überprüfen Sie, dass Ihre SAN-IOPS die Bedürfnisse der SQL-Datenbank erfüllen.

Siehe "Empfohlene Konfiguration für Notification Server mit lokal installierter SQL-Datenbank" auf Seite 67.

Siehe "Informationen zur Planung Ihrer SQL Server-Konfiguration" auf Seite 39.

Informationen über die Festlegung der Datenbankgröße für SQL Server

Sie können Richtlinien zur Größenfestlegung von Datenbanken verwenden, um die Leistung Ihres SQL Server-Computers zu optimieren. Eine Symantec Management-Plattforminstallation ohne Lösungen und verwaltete Computer führt zu einer Datenbankgröße von ungefähr 300 MB. Diese Größe beträgt ungefähr 7 Prozent der maximalen Datenbankgröße von SQL Express. Zusätzliche 500 verwaltete Computer können die Größe bis zu ungefähr 500 MB steigern. Datenbanken wachsen auch als Lösungen, die eingeführt und verwendet werden.

Sie bieten zwischen 750 KB und 1 MB Speicherplatz in der Datenbank für jeden verwalteten Computer. Die Festlegung der Größe berücksichtigt keine Datenbankfragmentierung über die Ersterstellung hinaus. Die tatsächlichen Größen variieren basierend auf den Lösungen, die installiert werden, und der speziellen Konfiguration von Richtlinien, Aufgaben und Zeitplänen. Die Datenbankwartungsstrategie, die Sie verwenden, beeinflußt auch Ihre Datenbankgröße.

Wenn Suiten in einer großen Umgebung installiert werden, kann die Datenbank auf bis zu 6 GB bis 12 GB wachsen. Wenn Sie eine Datenbankwachstumsstrategie wählen, müssen Sie ein Datenwachstum berücksichtigen.

Autogrow ist eine SQL Server-Einstellung, die Sie verwenden können, um bei unerwartetem Datenwachstum Unterstützung zu bieten. Verlassen Sie sich jedoch nicht auf autogrow, um Ihre Datenbankdateigrößen zu verwalten. Sie sollten die Dateien überwachen und sie entsprechend Ihrer prognostizierten Anforderungen während der Wartung in ihrer Größe ändern.

Um Ihre autogrow-Einstellung auszuwählen, schätzen Sie die erwartete maximale Größen der Datendatei und der Transaktionsprotokolldatei. Um diese Größe zu schätzen, können Sie das Wachstum dieser Dateien in einer Umgebung vor der

Produktion überwachen. Legen Sie das autogrow-Inkrement für Ihre Datendatei und Transaktionsprotokolldateien auf 10 bis 20 Prozent höher als Ihre erste Schätzung fest.

Verwenden Sie die autoshrink-Funktion nicht mit der Symantec Management-Plattform. Autoshrink wird regelmäßig im Hintergrund ausgeführt. Es verbraucht CPU- und E/A-Zyklen, die zu unerwarteten Leistungseinbußen führen können. Autoshrink kann die Datendateien fortwährend schrumpfen und erneut anwachsen lassen. Dieser Prozess verursacht eine Fragmentierung der Datenbankdatei. Diese Fragmentierung verschlechtert möglicherweise sequenzielle Übertragungen und willkürliche Zugriffe.

Nachdem Sie die ungefähre Größe der Datenbank geschätzt haben, sollten Sie eine Datenbankdatei dieser Größe erstellen, bevor Sie Notification Server installieren. Dieser Schritt stellt sicher, dass ausreichend Speicherplatz verfügbar ist. Er reduziert auch die negative Leistung einer Datenbank, die kontinuierlich wächst. Um Leistung weiter zu verbessern, sollten Sie die Datenbank nach seiner Erstinstallation defragmentieren und neu indexieren.

CMDB SQL Server sollte keine zusätzlichen Nicht-Symantec-Datenbankanwendungen hosten, weil die Symantec Management-Plattform sehr hohe Leistungsanforderungen stellt. Es können jedoch zusätzliche CMDB-Datenbanken auf dem gleichen SQL Server gehostet werden, weil jede Datenbank ähnliche Datenverkehrsanforderungen und Hardwarekonfigurationsanforderungen stellt.

Sie können über eine einzelne SQL-Instanz verfügen, die eine einzelne TempDB-Datenbank gemeinsam nutzt. Oder mehrere Datenbankinstanzen können jeweils über eine dedizierte TempDB-Datenbank verfügen. Mehrere Datenbankinstanzen minimieren das Risiko für potenziellen Konflikte, benötigen jedoch mehr Datenträgerarrays.

Eventuell sollte jede einzelne Datenbank jedes Notification Server-Computers auf einer separaten Instanz existieren. Eventuell sollen sie separate Instanzen sein, um TempDB-Datenbankkonflikte zu vermeiden.

Siehe "Informationen zur Planung Ihrer SQL Server-Konfiguration" auf Seite 39.

Info zur Arbeitsspeicherverwaltung für SQL Server

Die Arbeitsspeicherverwaltung ist ein wichtiger Teil der SQL Server-Leistungsoptimierung. Arbeitsspeicherverwaltung ist besonders wichtig, wenn SQL lokal auf den Notification Server-Computer ausgeführt wird.

Wenn Sie die x32-Version von SQL nutzen, sollten Sie die x64-Version des Betriebssystems nutzen.

x64 verarbeitet den vollständigen Adressraum, wohingegen x32 nur AWE und /3GB verwendet. Auf x32 ist die Verwendung des erweiterten Speichers durch SQL begrenzt, doch bei x64 kann SQL ihn vollständig für Pläne, Ergebniscache usw. verwenden.

Da x64 den vollständigen Adressraum verarbeitet, müssen Sie nicht PAE oder AWE verwenden. SQL Server 2008 x64 wird für dedizierte SQL-Server mit mehr als 4 GB physischem Arbeitsspeicher empfohlen.

Wenn Sie das Betriebssystem x32 verwenden müssen, überprüfen Sie, dass AWE richtig konfiguriert wird. Zum Beispiel /PAE, /3GB, die Berechtigung "Sperren von Seiten im Speicher" unter "Lokale Sicherheitsrichtlinie", die AWE-Einstellungen in SQL und die entsprechenden Einstellungen für den "MAX. SERVERARBEITSSPEICHER" in SQL. Das Sperren von Seiten im Speicher ist sowohl für 64-Bit- als auch für 32-Bit-SQL-Server geeignet und kann in der "Benutzerrechtzuweisung" der "Lokale Sicherheitsrichtlinie" gefunden werden.

http://msdn.microsoft.com/en-us/library/ms175581(v=sql.105).aspx

Wenn AWE auf x64 aktiviert ist. deaktivieren Sie es.

Tabelle 3-2 Konfigurationsoptionen des Arbeitsspeichers für SQL Server

Option	Beschreibung
Maximaler Serverarbeitsspeicher	Diese SQL-Einstellung begrenzt den Arbeitsspeicher, den SQL verbrauchen kann. Legen Sie den Wert "Maximaler Serverarbeitsspeicher" auf der Seite "Arbeitsspeicheroptionen für den Server" fest. Lassen Sie genügend Arbeitsspeicher, damit das Betriebssystem und Programme wie SQL Management Studio effizient ausgeführt werden können. Beispiel: ca. 4–6 GB weniger als der installierter RAM.
Arbeitsspeichernutzung unter Windows	Konfigurieren Sie die Arbeitsspeichernutzung unter Windows, sodass Programme gegenüber dem Systemcache den Vorrang erhalten. SQL Server verfügt über eine eigene Caching-Funktion zum Zwischenspeichen von Daten, um die Leistung zu verbessern.

Option	Beschreibung
Aktivieren Sie die Option "Für Ad-hoc-Arbeitsauslastungen optimieren".	Wenn die IT Management Suite verwendet wird, wird durch den alltäglichen Gebrauch der Symantec Management Console und die Hintergrundaktionen eine große Anzahl von Ad-hoc- oder dynamischen Abfragen generiert. Diese Typen von Abfragen werden unter Verwendung der Standardeinstellungen im Microsoft SQL Server nicht in den Cache-Speicher aufgenommen und können sich auf die Leistung der Console sowie des Notification Servers auswirken. Wenn die Option "Für Ad-hoc-Arbeitsauslastungen optimieren" aktiviert ist, wirkt sich das auch positiv auf den Plancache (oder auch Prozedurcache) aus. Wenn sie aktiviert ist, nimmt der SQL-Abfrageoptimierer einen ganzen Stapel zur Ausführung und versucht, einen entsprechenden Abfrageplan im Plancache zu lokalisieren. Wenn der SQL-Abfrageoptimierer keinen Abfrageplan findet, stellt er einen zusammen und speichert ihn im Cache, damit er beim nächsten Abrufen nicht erneut erstellt werden muss. Die Leistungszunahme findet statt, wenn die bestimmte Abfrage ein zweites Mal ausgeführt wird, da sie sich jetzt im Cache befindet. Es ist wichtig, zu verstehen, dass ein solcher Plan Platz im Arbeitsspeicher einnimmt und nicht auf Microsoft SQL-Servern implementiert werden sollte, die bereits verfügbaren Arbeitsspeicher maximieren. Diese Einstellung befindet sich auf der Seite "Erweitert" in den SQL Server-Instanz-Einstellungen innerhalb des Microsoft SQL Servers.

Siehe "Informationen zur Planung Ihrer SQL Server-Konfiguration" auf Seite 39.

Informationen zur Verwaltung der SQL-Datenbank

Ein SQL-Wartungsplan für die Neuerstellung von Indexen und Einstellen des freien Speicherplatzes für Indexe auf 10 % in den Symantec-/Altiris-Datenbanken sollte mindestens einmal im Monat (vorzugsweise wöchentlich) ausgeführt werden. Außerdem sollten durch diesen Wartungsplan die Spaltenstatistiken aktualisiert werden (Indexstatistiken werden während der Indexneuerstellung aktualisiert). Es wird empfohlen, diesen Plan während einer Zeit auszuführen, zu der die Datenbanknutzung von den Symantec-Anwendungen am niedrigsten ist. Dies kann beispielsweise an einem Sonntag oder während eines geplanten Wartungszyklus durchgeführt werden.

Folgen Sie diesen Empfehlungen für eine optimale Wartung von SQL:

- Aktualisieren der Statistiken (nachts)

- Dadurch wird sichergestellt, dass der Abfrageprozessor die optimale Auswahl für eine bestimmte ITMS-Implementierung durchführt.
- Stattdessen können Sie die Statistiken asynchron und automatisch aktualisieren.
  Arbeitsspeicherverlust in SQL – aktuelles Update durchführen
  Seite "Datenbankeigenschaften > Optionen".
  Eine Aktivierung kann sich auf das Versetzen einer Datenbank in den Einzelbenutzermodus (für Wartung) auswirken.

- Regelmäßige Wartung der Datenbankseite
  Neuerstellen der Indexe (monatlich)
  Neuorganisieren der Seiten (wöchentlich)
- Regelmäßiges Backup
  Modus zur einfachen Wiederherstellung – geringere Ein-/Ausgabe, aber aggressive Backup-Strategie erforderlich
  im Gegensatz zu VOLLSTÄNDIGE Protokollierung mit Backups

Weitere Informationen erhalten Sie in dem folgenden Supportdatenbank-Artikel:

http://www.symantec.com/docs/HOWTO8589

Verwenden des Microsoft SQL-Failover-Clustering mit ITMS 7.1 SP2 oder höher

Mit den folgenden Informationen wird das Failover-Clustering für Microsoft® SQL Server™ 2008 R2 beschrieben, eine Methode zum Erstellen von Hochverfügbarkeit für Ihre Symantec Management-Plattform (SMP). Das Failover-Clustering steht mit vollständigem Funktionsumfang in SQL Server 2008 R2 Enterprise und mit begrenzten Funktionen in der Standard Edition zur Verfügung.

Beim Failover-Clustering arbeiten das Betriebssystem und SQL Server 2008 R2 zusammen, um Verfügbarkeit im Falle von Anwendungs-, Hardware- oder Betriebssystemfehlern bereitzustellen. Das Failover-Clustering stellt Hardwareredundanz über eine Konfiguration zur Verfügung, in der unternehmenskritische Ressourcen automatisch von einem ausfallenden Computer zu einem gleichmäßig konfigurierten Datenbankserver übertragen werden.

Jedoch ist das Failover-Clustering keine Lastverteilungslösung. Failover soll nicht die Datenbankleistung verbessern, die erforderliche Wartung reduzieren, Ihr System gegen externe Bedrohungen schützen, nicht behebbare Softwarefehler, Single-Points-of-Failure (wie zum Beispiel nicht redundante(r) Speicher und Hardware) oder Naturkatastrophen verhindern.

Symantec empfiehlt, dass Sie genügend Kenntnisse von und Erfahrung mit Microsoft SQL-Failover-Methodologien haben, bevor Sie sie in einem ITMS oder in sonstiger

Suite oder Lösungsimplementierung versuchen möchten. Weitere Informationen zur Hochverfügbarkeit von SQL Server 2008 R2 finden Sie in der Dokumentation "High availability with SQL Server 2008 R2" unter der folgenden Adresse:

http://msdn.microsoft.com/en-us/library/ff658546(v=sql.100).aspx

Sie müssen auch berücksichtigen, dass Microsoft SQL Server die richtige Größe mit genügender Hardwarekapazität haben, um für die erwartete Failover-Arbeitslast adequat ausgeführt zu werden. Weitere Aspekte sind in der Dokumentation "Installing a SQL Server 2008 Failover Cluster" unter folgender Adresse zu finden:

http://msdn.microsoft.com/en-us/library/ms179410.aspx?

Das Failover-Clustering minimiert den ITMS-Systemausfall, indem es die CMDB hoch verfügbar macht. Das Failover-Clustering bietet Vorteile in den folgenden Szenarien:

- Hardwarefehler:
  Führen Sie Ihre SQL Server-Instanz einfach von einem anderen Knoten aus, während Sie Probleme auf dem anderen Knoten auflösen.
- Patchen/Warten von Server:
  Der SQL Server ist offline, während Sie auf den Neustart des Servers warten. Offline-Zeiten ermöglichen die Anwendung von Patches mit nur kurzen Systemausfällen für ITMS
- Problemlösung:
  Wenn ein Problem an einem der Knoten entsteht, ermöglicht das Failingover auf einen anderen Knoten die Fehlerbehebung einer Knotenkomponente, während ITMS weiterhin ausgeführt wird.

Gebräuchliche SQL Server-Failover-Methoden, die für ITMS zur Verfügung stehen

Dieser Abschnitt beschreibt die häufigsten Failover-Cluster-Konfigurationen und wie sie auf ITMS zutreffen:

Einzelinstanz-Failover-Cluster

Ein Einzelinstanz-Failover-Cluster besteht aus mindestens zwei Einzelknoten-SQL-Servern, die eine allgemeine Speicherquelle gemeinsam nutzen. Nur ein SQL Server-Knoten ist jederzeit aktiv, alle weiteren Knoten des Clusters befinden sich im Wartezustand. In unserem Beispiel wird der Notification Server an das SQL-Cluster angehängt und kann auf seine CMDB zugreifen. Der Notification Server erkennt Knoten 1 oder Knoten 2 nicht und erachtet den SQL-Cluster als seinen Verbindungspunkt.

Abbildung 3-1 zeigt einen Cluster mit zwei Knoten an. Dies ist die gebräuchlichste Konfiguration für in ITMS verwendeten SQL-Failover. Diese Anordnung ermöglicht

es einem dedizierten Computer, sich vor dem Ausfall eines einzelnen Knotens im Cluster zu schützen. Symantec empfiehlt, dass alle Knoten in dieser Konfiguration dieselbe SQL Server-Hardware haben. Dadurch wird konsistente Leistung bei einem Failover sichergestellt. Wenn Bedarf für zusätzliche Failover-Redundanz besteht, können Sie die Anzahl der Knoten innerhalb des Clusters erhöhen. SQL Server 2008 R2 Standard Edition unterstützt den Failover von zwei Knoten, während die Enterprise Edition bis zu 16 Knoten ermöglicht. Microsoft SQL Server-Lizenzen sind nur auf dem aktiven Knoten innerhalb des SQL-Clusters erforderlich.

Abbildung 3-2 zeigt einen kritischen Failover des aktiven SQL-Knotens an. Wenn ein kritischer Ausfall des aktiven SQL Server-Knotens auftritt, übernimmt der zweite Knoten die Aufgaben des ersten Knotens. Notification Server wird von der CMDB getrennt, bis Knoten 2 eine Verbindung zur CMDB herstellt. Sobald Knoten 2 aktiv ist, kann Notification Server eine Verbindung herstellen und der Betrieb wird fortgesetzt. Während des Verbindungsabbruchs sind Dienste, Konsole, Aufgabe und andere Verwaltungelemente nicht verfügbar. Die Failover-Verzögerung hängt von verschiedenen Faktoren ab, wie zum Beispiel von der Konnektivität, der Datenbankgröße und der Anzahl der SQL-Datenbanken im Cluster. Idealerweise sollte der Failover in weniger als 30 Minuten auftreten.

Abbildung 3-1 SQL-Clusterkonfiguration mit zwei Knoten

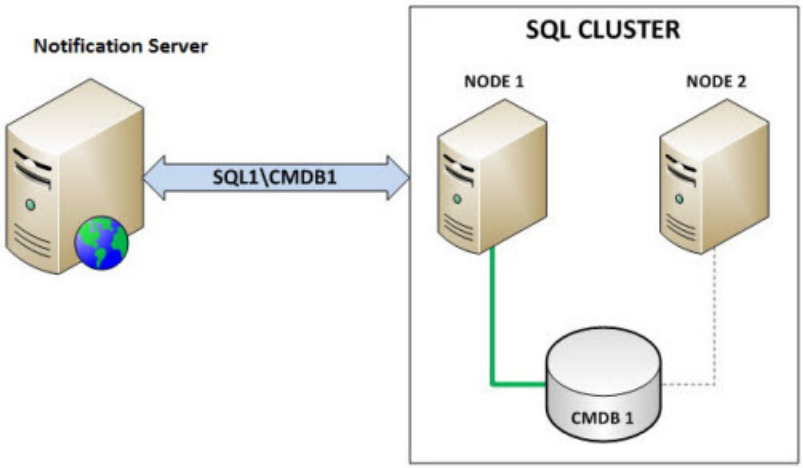
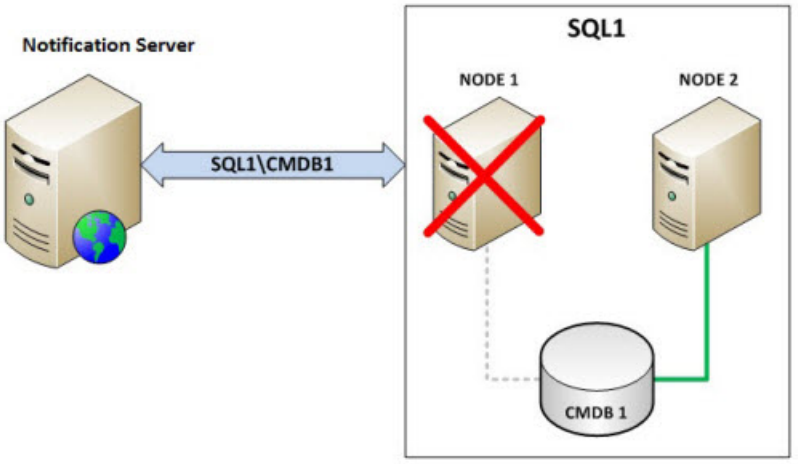


Abbildung 3-2 Failover des aktiven SQL Server-Knotens in einem SQL-Cluster mit zwei Knoten



Hinweis: Wird SQL für IT Analytics verwendet, ist Analysis Services clusterfähig, Reporting Services jedoch nicht. Wenn der Knoten mit Reporting Services ausfällt, fällt auch IT Analytics aus, bis der primäre Knoten wiederhergestellt wird.

Mehrfachinstanz-Failover-Cluster

Die häufigsten Typen von Mehrfachinstanz-Clustern sind jene, bei denen alle Knoten eine oder mehrere Failover-Cluster-Instanzen ausführen.

Abbildung 3-3 zeigt eine SQL-Umgebung mit einzelnem Cluster an, mit deren Hilfe zwei separate Instanzen der CMDB für Notification Server 1 und Notification Server 2 gehostet werden, wobei jede CMDB auf einem separaten physischen Knoten ausgeführt wird. Während diese Konfiguration in Betrieb ist, greifen beide Notification Server mit der vollen Leistung ihrer jeweiligen Knoten auf ihre CMDB zu.

Abbildung 3-4 zeigt an, wie alle Failover-Cluster-Instanzen, die der Knoten hostet, bei Ausfall eines Knotens den Failover auf einen anderen Knoten ausführen. Knoten 1 ist fehlgeschlagen und CMDB 1-Failover wird auf Knoten 2 ausgeführt. Während des Failovers wird der Notification Server von der CMDB getrennt, bis Knoten 2 den Failover-Betrieb abgeschlossen hat und CMDB 1 bereitstellt. Notification Server 1 stellt wieder eine Verbindung her und arbeitet mit reduzierter Leistung, bis Knoten 1 in einem betriebsfähigen Zustand ist. Die Leistung von Notification Server 2 wird auch beeinträchtigt, da er zu diesem Zeitpunkt zwei CMDBs hostet.

Mit der richtigen SQL Server-Größe ermöglicht diese Methode ein hohes Maß an Datenbankreaktionsfähigkeit und -leistung sowie eine produktive Nutzung Ihrer wertvollen Hardware. Microsoft SQL Server-Lizenzen sind auf allen aktiven Knoten in dieser Implementierung (in diesem Fall alle Knoten im Microsoft SQL-Cluster) erforderlich.

Abbildung 3-3 SQL-Konfiguration mit einzelnem Cluster, die zwei CMDB-Instanzen hostet

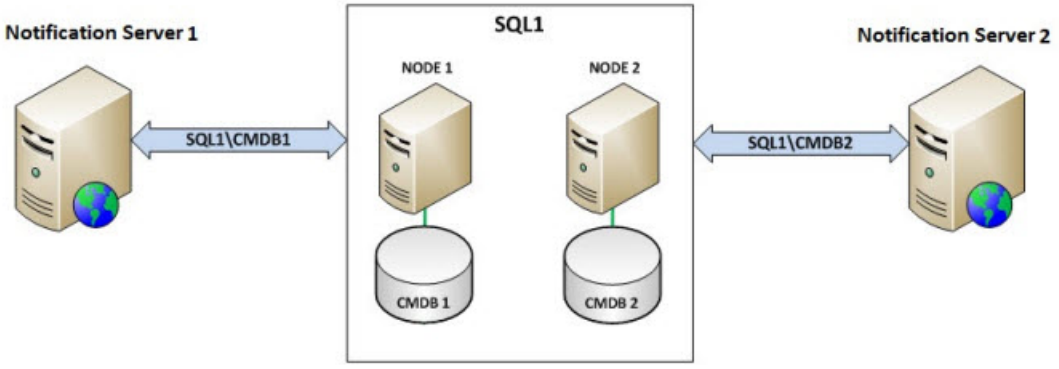
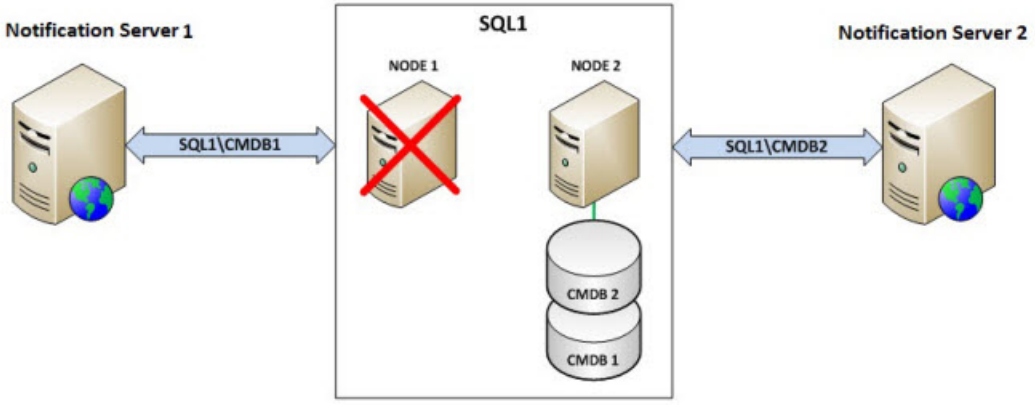


Abbildung 3-4 Failover-Cluster-Instanzen, die Knoten 1 hostet, führen einen Failover auf Knoten 2 aus



Siehe "Informationen zur Planung Ihrer SQL Server-Konfiguration" auf Seite 39.

Informationen zur Planung Ihrer Site Server

Eine Site ist ein Verwaltungskonstrukt, mit dem Sie Subnetze Site Services zuordnen können. Site Services sind eine Erweiterung des Symantec Management Agents. Wenn ein Site Service auf einem verwalteten Knoten installiert wird, stuft er den Symantec Management Agent zu einem Site Server hoch.

Aufgabe, Paket und Netzwerkstartdienste sind alles Site Server-Rollen. Diese Site Services können in mehreren Kombinationen bereitgestellt werden, um die Anforderungen von Endgeräten zu erfüllen. Eine Remote-Site benötigt möglicherweise nur einen Package Server oder einen Netzwerkstartserver. Ein Task Server wird eventuell nur im Rechenzentrum benötigt. Ihre Topologie und Ihr Einsatz von Lösungen bestimmt, ob Sie Site Services auf einen einzelnen Computer kombinieren oder dedizierte Computer verwenden sollen.

Die Standardinstallation des Notification Servers erfüllt nur die Mindestanforderungen von Site Servern. Site Server verwenden möglicherweise das Betriebssystem "Windows Workstation" oder ein "Windows Server". Für eine Site mit weniger als 100 Endgeräten sind möglicherweise nur 10 Sitzungen erforderlich. Für größere Remote-Standorte ist jedoch eventuell ein Windows-Server erforderlich.

Ihre primäre Erwägung für die Hardware und das Betriebssystem des Site Servers besteht in der Anzahl von gleichzeitigen Sitzungen, die Sie benötigen. Windows Workstation ist auf 10 gleichzeitige TCP-Verbindungen begrenzt. Windows Server weist nicht dieselben Beschränkungen auf.

Falls Sie einen Site Service auf einem Windows 7/2008-Computer installieren, müssen Sie die Dienste mit IIS 6-Kompatibilitätsmodus darauf installieren.

Siehe "Informationen zum Paketdienst" auf Seite 57.

Siehe "Informationen zum Task Service" auf Seite 53.

Siehe "Info zum Netzwerkstartdienst" auf Seite 58.

So planen Sie ein Site-Design

Folgende Empfehlungen sollten Sie beim Planen eines Site-Designs in Erwägung ziehen:

- Planen, designen, konfigurieren und überwachen Sie Sites für die Integrität der Site.
  In allen Infrastrukturen sollten Sie bei der Planung, dem Design, der Konfiguration und der Überwachung Wartungsarbeiten mit einplanen.
- Bevorzugen Sie Sites und Organisationsgruppen gegenüber der Hierarchie.
  Verlassen Sie sich für die Verwaltung von Implementierungen an verschiedenen Standorten nicht ausschließlich auf die Hierarchie. Verwenden Sie dafür

stattdessen Site Server. Ihr Design sollte den Anforderungen an die Bandbreite und die Gesamtknotenzahl entsprechen.

- Verwenden Sie eingeschränkte Package Server und stellen Sie Ihre Pakete stufenförmig bereit.
  Sie können eingeschränkte Package Server als primäre Methode verwenden, um sicherzustellen, dass die Kommunikation wie erwartet stattfindet. Doch einige wichtige Agent-Kommunikationen finden direkt mit dem ITMS-Server statt. Dazu gehören beispielsweise GetPackageInfo, CreateResource, PostEvent, etc.
  Bei der stufenförmigen Paketbereitstellung sollte der Agent die Berichte an den eingeschränkten Package Server senden. Der eingeschränkte Package Server sollte die Berichte an den uneingeschränkten Package Server senden.
- Beschränken Sie die Task Server-Kommunikation auf dem ITMS-Server.
  Stellen Sie anstelle von Bandbreitenkonsolidierung Verbindungsverwaltung und Anfragenkonsolidierung bereit.
  Stellen Sie keine Verbindung zwischen Agent und übergeordneter Instanz her. Im Allgemeinen sollten Sie mindestens über einen Task Server verfügen.

Weitere Informationen erhalten Sie in den folgenden Quellen:

- Task Server – Bewährte Verfahren
- Bereitstellungsverfahren für Pakte
- Konfigurieren des eingeschränkten Package Servers:
- Eingeschränkter Package Server
- Package-Replikation in einer Hierarchie

Siehe "Informationen zur Planung Ihrer Site Server" auf Seite 51.

Info zur Site-Verwaltung

Unter Standortwartung versteht man die Verwaltung der Standorte, Subnetze und Site Services in Ihrer Organisation. Sie können Ihre Computer entsprechend dem Standort und Subnetz verwalten, wodurch Sie Gruppen von Computern steuern und dabei den Bandbreitenverbrauch minimieren können. Ein Standort ist üblicherweise ein physischer Standort in Ihrer Organisation (beispielsweise ein bestimmtes Gebäude bzw. die Etage eines Gebäudes). Ein Subnetz ist ein Bereich logischer Adressen in Ihrem Netzwerk.

Unter normalen Betriebsbedingungen wartet jeder Package Server oder Task Server nur die Symantec Management-Agents, die innerhalb der zugewiesenen Standorte vorhanden sind. Wurde keine Standorte definiert, stehen alle Site Server für die Wartung aller Symantec Management-Agents zur Verfügung (obwohl dies nicht empfohlen ist).

Wurden keine Standorte für einen Package Server oder Task Server definiert, verwendet der Notification Server die folgenden Regeln:

- Notification Server versucht zuerst, Site Server auf demselben Subnetz zu finden, auf dem sich der anfordernde Computer befindet. Wenn Site Server gefunden werden, werden diese an den Symantec Management-Agent zurückgegeben.
- Wenn keine Site Server sich im gleichen Subnetz wie der anfordernde Computer befinden, werden alle Site Server an den Symantec Management-Agent zurückgegeben.
- Wenn keine Site Server verfügbar sind, wird der Agent an den Notification Server-Computer verwiesen.

Sie können Site Server mit Hilfe der folgenden Methoden Standorten zuweisen:

- Weisen Sie das Subnetz zu, das den Site Server für einen Standort enthält.
- Weisen Sie den Site Server einem Standort zu.
- Verwenden Sie den Connector für Active Directory, um die Aufgabe durchzuführen.
  Der Connector für Active Directory überschreibt Subnetze und Standorte, die Konflikte verursachen. Beispiel: Wenn Sie Subnetze manuell einem Standort zuweisen, der in Konflikt zu dem steht, was sich im Connector für Active Directory befindet, werden die Active Directory-Informationen verwendet.

Nachdem die Liste der verfügbaren Site Server an den Symantec Management-Agent zurückgegeben wurde, wählt der Agent den am besten geeigneten Site Server.

Site Server und verwaltete Computer können über mehrere Netzwerkkarten und IP-Adressen verfügen und deshalb durch Subnetzzuweisung zu mehr als einem Standort gehören.

Informationen zum Task Service

Aufgabenkommunikation ist im Gegensatz zur Richtliniekommunikationen einmalig. Verwaltete Computer starten die Richtlinienkommunikation, und der Server startet die Aufgabenkommunikation.

Sie können mit dem Task Service folgende Schritte durchführen:

- Mehrere Aufgaben in einer definierten Reihenfolge ausführen, die als Job bezeichnet wird.
- Logik für die Verarbeitung von Aufgabenfehlern oder andere Rückgabecodes zur Verfügung stellen.

- Kommandozeilen- und VBscript-Funktionen für verwaltete Computer bereitstellen.
- Standardisierte Energieverwaltung bereitstellen.
- Clientseitige und serverseitige Aufgaben ausführen.
- Aufgaben in mehreren Jobs wieder verwenden. Aufgaben können nach Bedarf geklont und geändert werden.

Symantec empfiehlt mindestens einen Task Server pro Notification Server. Für Aufgaben ist eine hohe Leistung des Notification Server-Prozessors sowie Speicher erforderlich, weil er regelmäßig Tickle-Pakete senden und den Ausführungsstatus abrufen muss. Diese Anforderung kann sich auf das Laden von SQL-Daten und die Reaktionsbereitschaft der Benutzeroberfläche negativ auswirken. Sie können die Verarbeitung von Aufgaben an einen Task Server auslagern. Ein dedizierter Server verarbeitet die Agent-Tickle-Kommunikation, die Aufgabensequenzierung und die Automatisierungsfunktionen. Die Verteilung von Aufgaben an einen Task Server reduziert die Last auf dem Notification Server. Die Last wird reduziert, indem die Unterbrechung zum Notification Server minimiert wird.

Siehe "Informationen zur Planung Ihrer Site Server" auf Seite 51.

Task Server verwenden eine hohe Anzahl von Betriebssystemsitzungen. Wenn ein Task Server mehr als 100 verwaltete Computer unterstützt, wird ein Windows Server-Betriebssystem empfohlen. Verwenden Sie das Windows Server-Betriebssystem, weil es viel mehr gleichzeitige Betriebssystemsitzungen unterstützt. Wenn ein Task Server weniger als 100 verwaltete Computer unterstützt, wäre möglicherweise ein Workstation-Betriebssystem ausreichend. Der Task Server-Computer muss auch die Funktionen "IISs 6.0" oder "IISs 7.0" und ".NET Frameworks 3.5." aktiviert haben.

Für Task Server ist keine leistungsstarke Hardware erforderlich. Ein moderater Geschwindigkeitsprozessor ist ausreichend. Datenträger-E/A ist kein bedeutender Faktor bei der Task Server-Leistung. Jedoch kann die Aufgabenkommunikation mehrere gleichzeitige Verbindungen zum Task Server verbrauchen. Eine Windows-Arbeitsstation ist nur auf 10 gleichzeitige TCP-Verbindungen begrenzt und ein Windows Server-Betriebssystem weist nicht dieselben Beschränkungen auf. Deshalb ist möglicherweise ein Windows Server-Betriebssystem auf Ihrem Task Server erforderlich. Symantec empfiehlt ein Windows Server-Betriebssystem für die Task Server, die mehr als 100 verwaltete Computer unterstützen.

Task Server sind für das Auslagern von Leistungsanforderungen vom Notification Server sehr gut geeignet. Sie sind nicht dafür ausgelegt, Netzwerkbandbreitenbeschränkungen zu beheben. Sie können einen Task Server in das gleiche Subnetz wie Notification Server stellen, da er wenig Einfluss auf die Minimierung des Netzwerkverkehrs hat.

Verwenden Sie die folgenden Richtlinien, um Task Services innerhalb Ihrer Infrastruktur zu konfigurieren:

- Symantec empfiehlt mindestens einen Task Server pro Notification Server. Nach dem ersten dedizierten Task Server müssen Sie zusätzliche Task Server für jeweils 5.000 bis 7.500 Endgeräte hinzufügen.
- Sie können die Last auf mehrere Task Server innerhalb großer Sites aufteilen, um sicherzustellen, dass Agents über die aktuellste Aufgabenausführung verfügen.
- Sie können die Last auf Task Servern reduzieren, wenn Sie die Einstellungen "Intervall für Aufgabenaktualisierung" und die maximale Zeit zwischen Tickle-Ereignissen erhöhen. Standardmäßig werden diese auf alle 5 Minuten festgelegt. Sie sollten diese Einstellungen auf einen Wert größer als 10 Minuten ändern.
- Sie müssen die Siteverwaltung verwenden, um Computer zu zwingen, den Task Server zu verwenden, falls sich der Notification Server und der Task Server in der gleichen Site befinden.
- Um sicherzustellen dass der Task Server richtig installiert und konfiguriert wird, installieren Sie den Aufgabendienst über die Symantec Management Console.

Wie Task Server die Tickle-Funktion verwendet

Der Tickle-Server ist eine Komponente von Task Management. Diese Komponente wird nur auf dem Notification Server ausgeführt und ist dafür verantwortlich, Task Server von bevorstehenden Aufgaben für ihre Clientcomputer zu unterrichten. Task Server haben auch die systemeigene Fähigkeit, Tickles an ihre registrierten Clientcomputer zu senden. Diese Tickle-Funktion unterscheidet sich vom Tickle Server auf dem Notification Server-Computer.

Der Tickle Server sendet ein IP-Tickle-Paket an Task-Server, wenn einer seiner registrierten Clientcomputer einen Auftrag oder eine Aufgabe auszuführen hat. Nach Empfang des Tickle-Pakets fordert der Task Server sofort die Aufgaben- oder Auftragsinformationen vom Notification Server für seine registrierten Clientcomputer an. Er sendet auch Tickles an seine Clientcomputer. Wenn der Client Task Agent das Tickle-Paket empfängt, fordert er die Auftrags- oder Aufgabeninformationen von seinem registrierten Task Server an. Die Aufgabe wird erst ausgeführt, nachdem der Client Task Agent die Aufgabeninformationen erhält. Statusereignisse für vollständige Aufgaben werden nach Beendung an den registrierten Task Server zurückgesandt.

Wenn die Tickle-Pakete blockiert sind oder ihr Ziel sonst nicht erreichen können, richtet sich der Client Task Agent automatisch an seinen registrierten Task Server, um neue Jobinformationen anzufordern. Er führt diese Prüfung alle 5 Minuten aus.

Dieses Intervall zur Aufgabenanforderung kann in der Symantec Management Console konfiguriert werden. Task Server-Aufgaben- und Auftragsinformationen werden nicht durch die Konfigurationsrichtlinie des Symantec Management-Agent empfangen. Der Client Task Agent empfängt sie direkt von seinem registrierten Task Server. Wenn Sie den Symantec Management-Agent zur Aktualisierung seiner Konfigurationsrichtinie zwingen, wird der Empfang von Informationen über bevorstehende Aufgaben durch den Client Task Agent nicht erzwungen.

Standardmäßig verwendet der Tickle Server Port 50123 für Task Server, und Task Server verwenden Port 50124, um Client Task Agents Tickles zu senden.

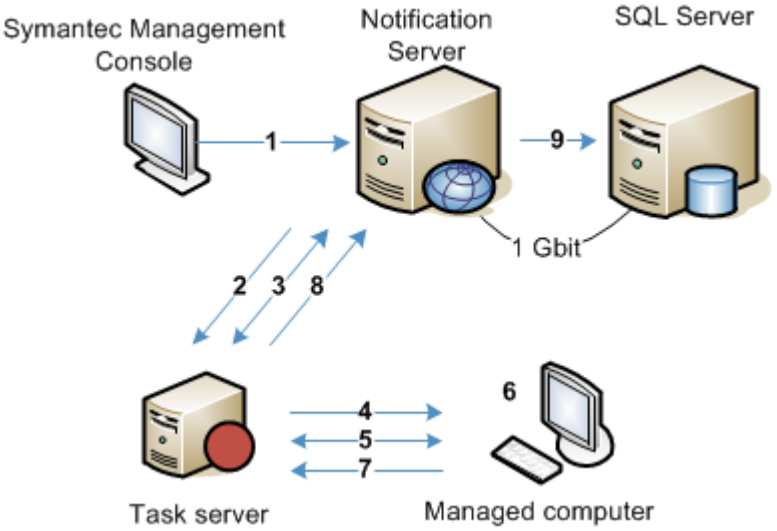
Im folgenden Beispiel wird angenommen, dass der Client Task Agent für ComputerA mit RemoteTaskServer1 registriert ist.

Tabelle 3-3 Reihenfolge, in der der Task Server Tickle verarbeitet

Reihenfolge	Beschreibung
Eins	Ein Notification Server-Administrator weist eine Aufgabe zu, die sofort auf ComputerA ausgeführt werden soll.
Zwei	Der Tickle Server auf dem Notification Server-Computer sendet ein Tickle-Paket, um RemoteTaskServer1 von der bevorstehenden Aufgabe zu unterrichten.
Drei	RemoteTaskServer1 prüft, ob der Zielclient beliebige Aufgaben erhalten darf. Ist der Modus "Legacy-Agent-Kommunikation" deaktiviert und ist das Ziel ein Legacy-Agent, schlägt die Aufgabe sofort fehl. Sie schlägt auch fehl, wenn der Agent aktualisiert wird, sich aber im Zustand "Nicht zulässig" befindet. Siehe "Info zu Agent-Registrierung" auf Seite 61.
Vier	RemoteTaskServer1 empfängt das Tickle-Paket und fordert sofort die Auftragsinformationen vom Notification Server an.
Fünf	RemoteTaskServer1 sendet Tickles an ComputerA, um diesen von der bevorstehenden Aufgabe zu unterrichten.
Sechs	ComputerA empfängt das Tickle-Paket und fordert sofort die Auftragsinformationen von seinem registrierten Task Server (RemoteTaskServer1) an.
Sieben	ComputerA empfängt die Auftragsinformationen und führt die Aufgabe aus.
Acht	Nach Abschluss der Aufgabe sendet ComputerA ein Statusereignis zurück an RemoteTaskServer1.

Reihenfolge	Beschreibung
Neun	RemoteTaskServer1 speichert das Statusereignis zwischen und versucht sofort, es an den Notification Server weiterzuleiten.
Zehn	Notification Server empfängt das Statusereignis vom RemoteTaskServer1 und zeichnet die Informationen in der Datenbank auf.

Abbildung 3-5 Reihenfolge, in der der Task Server Tickle verarbeitet



Informationen zum Paketdienst

Package Server sind die Bereitstellungmechanismen, mit denen Daten effizient in eine Site verschoben werden. Sie funktionieren mit Notification Server als lokale Dateiserver für verwaltete Computer auf einer Site. Für Package Server sind keine Hardware und Software der Serverklasse erforderlich.

Mit Package Servern können Sie den Netzwerkverkehr reduzieren, indem sie es ermöglichen, dass ein Paket nur einmal pro Site über das Netzwerk kopiert wird. Sie können einen Package Server auf einer Site lokal ablegen, um Pakete zu speichern und bereitzustellen. Diese Architektur kann Ihnen helfen, Sites mit Verbindungen geringer Bandbreite zum Notification Server zu verwalten.

Siehe "Informationen zur Planung Ihrer Site Server" auf Seite 51.

Wenn Sie ein Paket auf Notification Server aktivieren, wird er auf alle Package-Server kopiert, die Notification Server kennt. Sobald die Kopie erfolgreich ist, laden verwaltete Computer die Pakete vom lokalen Package Server anstelle vom standortfernen Notification Servers herunter.

Die Anzahl von Package Servern, die Sie benötigen, richtet sich nach Ihrer Netzwerktopologie und Bandbreite. Sie hängt auch von der Größe Ihrer Pakete und von der Häufigkeit der Pakete ab, die bereitgestellt werden sollen.

Sie können die Bereitstellung von Paketen auf den Package Servern staffeln, um die Last zu reduzieren. Sie können jeweils eine beschränkte Anzahl Pakete für alle Package Server bereitstellen. Sie können auch nur für eine ausgewählte Gruppe Package Server Pakete bereitstellen.

Ein eingeschränkter Package Server kann nur innerhalb der Sites funktionieren, denen er zugewiesen ist. Ein uneingeschränkter Package Server kann von überall im System Pakete und andere Ressourcen beziehen. Der uneingeschränkte Package Server erfasst alle erforderlichen Ressourcen von außerhalb der Site und stellt sie allen eingeschränkten Package Servern zur Verfügung. Ein Site Server kann nur dann als Package Server funktionieren, wenn mindestens ein uneingeschränkter Package Server vorhanden ist, der ihm zugewiesen ist. Es muss mindestens ein uneingeschränkter Package Server in einer Site mit einen oder mehreren eingeschränkten Package Servern vorhanden sein.

Info zum Netzwerkstartdienst

Ein Startserver im Netzwerk soll PXE-Startdienste und Boot-Pakete für Netzwerksegmente bereitstellen. Am häufigsten wird er verwendet, um ein Standard-Image zu Support-Zwecken wiederherzustellen oder um in einer Ersteinrichtung neue Computer zu installieren. Gewöhnlich wird das PXE-Potokoll in einem Netzwerk gesteuert. Es kann auf ein Subnetz oder einen anderen auf IP-Hilfsfunktionen basierenden Bereich beschränkt werden. Wenn für viele Systeme gleichzeitig neue Abbilder erstellt werden müssen, können Sie in jedem Netzwerksubnetz Startserver im Netzwerk platzieren und in einem großen Subnetz weitere hinzufügen. Ein Startserver im Netzwerk stellt nicht nur PXE-Dienste bereit, sondern hostet ähnlich wie ein Package Server Pakete, die als Startabbild bezeichnet werden.

Siehe "Informationen zur Planung Ihrer Site Server" auf Seite 51.

Jedes Subnetz muss Zugriff auf einen Startserver im Netzwerk haben. Allerdings blockieren Router in der Regel PXE-Proadcast-Pakete.

Sie können die folgenden drei Methoden verwenden, um jedem Subnetz Zugriff zu gewähren:

- Verwenden Sie die DHCP-Erzwingung, die PXE-Anforderungen von Clients an den nächsten Startserver im Netzwerk weiterleitet. Diese Methode funktioniert selbst dann, wenn sich der Client-Computer in einem anderen Subnetz als der Netzwerkstartserver befindet. DHCP ermittelt mithilfe der Subnetzmaske und Ping-Tests den richtigen Server.
- Verwenden Sie die Einstellung “IP Helpers”, die Sie bei jedem Router konfigurieren können, um PXE-Anforderungen zwischen Subnetzen weiterzuleiten.
- Installieren Sie auf jedem Subnetz einen Netzwerkstartserver. Diese Methode wird nicht empfohlen, weil sie unnötigen Overhead erzeugt.

Ein Startserver im Netzwerk enthält die folgenden Objekte:

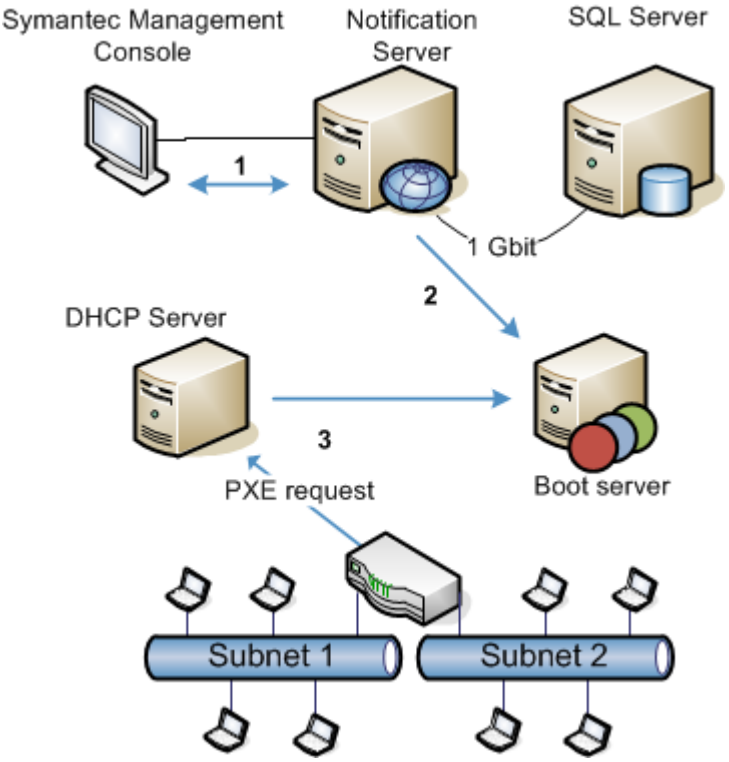
- PXE-Dienst
- Boot-Images
- Die NSCap- oder Package Server-Freigabe mit den Imagingprogrammen, wenn die Programme kein Teil des Preboot-Images sind.
- Die Treiberdatenbank

Wenn auf ein vorhandenes Startabbild neue Einstellungen angewendet werden, wird lokal auf jedem Startserver im Netzwerk ein aktualisiertes Startabbild zusammengestellt. Diese Änderungen werden mithilfe einer Richtlinie bereitgestellt und hängen vom Aktualisierungszeitplan des Symantec Management-Agent ab.

Tabelle 3-4 Folge für die Konfiguration des Startservers im Netzwerk

Schrittfolge	Beschreibung
Eins	Deployment Solution wird auf dem Notification Server-Computer installiert. Der Administrator konfiguriert und verwaltet Deployment-Aufträge und Aufgaben von der Symantec Management Console aus.
Zwei	Der Administrator aktiviert und konfiguriert den Netzwerkstartdienst.
Drei	Der DHCP-Server kann PXE-Anfragen von den Client-Computern an die Startserver im Netzwerk weiterleiten, die sich auf mehreren Subnetzen befinden.

Abbildung 3-6 Folge für die Konfiguration des Startservers im Netzwerk



Symantec Management Agent-Bereitstellungsplanung

In einigen Umgebungen werden Computer mit einem Unternehmens-Software-Image oder einer Standardbasisliste mit Software eingerichtet. Wenn Sie das Agent-Image dem Computer-Image hinzufügen, können Sie Zeit und Aufwand sparen. Der Symantec Management Agent kann vorinstalliert und in einem Verzeichnis mit einer Betriebssystemrichtlinie "Einmal ausführen" abgelegt werden.

Siehe "Informationen über die Leistungsoptimierung des Symantec Management Agents" auf Seite 113.

Sie können Skiptmechanismen auch zum Installieren des Agents verwenden. Sie können eine Push-Operation des Symantec Management Agents von der Symantec Management Console ausführen, wenn Sie den Agent keinem Image-Build hinzufügen möchten.

Für die Push-Methode ist ein geringeres Eingreifen von Außen erforderlich als bei anderen Methoden der Agent-Bereitstellung auf Computern, die bereits im Einsatz

sind. Mit dieser Methode kontaktiert der Notification Server den Clientcomputer, und der Clientcomputer fordert dann den Agent vom Notification Server an. Für die Push-Methode müssen Sie die Dateifreigabe-Einstellung deaktivieren.

Sie können den Agent mit der aktivierten Dateifreigabe weiterhin bereitstellen. Der Clientcomputer kann diese Anforderung weiterhin selbstständig initiieren. Beispielsweise kann bei E-Mail entweder ein Skript versendet werden, oder ein Web-Link kann zum Abrufen des Agents gesendet werden.

Info zu Agent-Registrierung

Bei der Funktion für Agent-Registrierung ist erforderlich, dass ein Clientcomputer für die Kommunikation mit dem Notification Server zugelassen ist, bevor er von diesem Notification Server verwaltet werden kann. Die Standardrichtlinie für Agent-Registrierung ermöglicht allen Computern eine Kommunikation mit dem Notification Server. Sie können jedoch auch benutzerdefinierte Richtlinien für die Agent-Registrierung erstellen, durch die bestimmte Computer zugelassen oder blockiert werden können.

Nachdem durch die Richtlinie für Agent-Registrierung ein Computer zugelassen oder blockiert wurde, können Sie anschließend den Status nur manuell auf der Berichtsseite "Agent-Registrierungsstatus" ändern. Beispielsweise können Sie Computer, die im ausstehenden Status sind, zulassen oder blockieren. Außerdem können Sie die Registrierung der Agents, die Sie zuvor zugelassen haben, widerrufen.

Agent-Registrierung wird auf Windows-, UNIX-, Linux- und Mac-Plattformen unterstützt.

Kapitel 4

Hardwareempfehlungen

In diesem Kapitel werden folgende Themen behandelt:

- Empfohlene Hardware für die IT Management Suite 7.5
- Empfohlene Internet-Gateway-Hardware
- Empfohlene Konfiguration für Notification Server mit lokal installierter SQL-Datenbank
- Empfohlene maximale Computeranzahl für IT Management Suite 7.5
- Unterstützte Betriebssysteme für Notification Server und Site Server
- Info zu unterstützten SQL Server-Kollatierungen
- Durch Symantec Installation Manager installierte IIS Rollen-Dienste
- SQL Server-Empfehlungen und Drittanbietersoftware-Anforderungen

Empfohlene Hardware für die IT Management Suite 7.5

Bestimmen Sie Ihre Hardwareanforderungen anhand der Empfehlungen in diesem Thema. Im Folgenden finden Sie allgemeine Empfehlungen zur Hardware für die meisten Umgebungen mit IT Management Suite 7.5. Je nach spezifischen Gegebenheiten kann die entsprechende Hardware variieren.

Erwägungen zum virtuellen Computer (VM)

ITMS hat" Aktivitäten "Burst" um Zeitpläne und entsprechende Datenverarbeitung. Eine Grund für Ausfälle in den Umgebungen ist, dass Speicheradministratoren Ressourcen entfernen, weil die Baselines eventuell keine kontinuierliche Notwendigkeit für Ressourcen anzeigen. Jedoch sollten die Ressourcen weiterhin verfügbar sein, um auch Aktivitätsspitzen zu bearbeiten.

Beachten Sie die von der VM-Umgebung verursachte Latenz. Latenz kann von Sachen wie unzulänglichem Arbeitsspeicher, langsame Konfigurationen von Datenträgersubsystem, Gebrauch oder übermäßige Verwendung von Snapshots, ungenügende CPUs und vielen anderen Faktoren verursacht werden, die die Fähigkeit der VMs, die Ressourcen zu erhalten, wenn sie erforderlich sind, betreffen können.

VM-Latenz entsteht meistens durch eine zu hohe Anzahl von Abonnements der Ressourcen auf. Sie kann aber auch durch andere Faktoren entstehen, wie vMotion-Stürme oder Stürme von ähnlichen Ressourcen, falsche Konfiguration und bei manchen Speichersystemen sogar die Verwendung von Snapshots, die wegen MBR-Ausrichtproblemen zwischen VMware und dem Speicheranbieter übermäßiges Schreiben verursachen.

Hardwareempfehlungen

Hinweis: Diese Empfehlungen sind KEINE Mindestanforderungen. Das Implementieren dieser Empfehlungen sollte eine angemessene Leistung von Notification Server für Inventarerfassung und Antwortzeiten der Benutzeroberfläche gewährleisten.

Tabelle 4-1 Hardwareempfehlungen für Microsoft SQL Server

Komponente	Auswertung (1 - 20 Endgeräte)	100 - 1.000 Endgeräte	1,000 - 5,000	5.000–10.000	10.000 - 20.000 Endgeräte
Prozessoren/ Geschwindigkeit	Zwei Cores/2,4 Ghz oder mehr	Vier Cores/2,4 Ghz oder mehr	Acht Cores/2,4 Ghz oder mehr	8 - 16 Cores/2,4 Ghz oder mehr	16 und mehr Cores/2,4 Ghz oder mehr
Datenträger-geschwindigkeit (in den IOPS)	180 - C: Betriebssystem, SMP 200 - D: SQL	180 - C: Betriebssystem, SMP 200 - D: SQL	180 - C: Betriebssystem, SQL App 300 - D: SQL DB 300 - E: Protokolle 200 - F: TempDB	180 - C: Betriebssystem, SQL App 400 - D: SQL DB 400 - E: Protokolle 300 - F: TempDB	180 - C: Betriebssystem, SQL App 600 - D: SQL DB 600 - E: Protokolle 400 - F: TempDB
Plattenkapazität	80 GB	80 GB	120 GB	250 GB	400 GB
RAM	16 GB	16 GB	16+ GB	24+ GB	32+ GB
Cache	6MB L2 oder mehr				
Netzwerk	Dual Gigabit - mit Lastverteilung				

Komponente	Auswertung (1 - 20 Endgeräte)	100 - 1.000 Endgeräte	1,000 - 5,000	5.000–10.000	10.000 - 20.000 Endgeräte
Betriebssystem	Windows Server 2008 R2 SP1 x64 Standard Edition				

Tabelle 4-2 Empfehlungen für physische und virtuelle Hardware für Notification Server

Komponente	Auswertung (1 - 20 Endgeräte)	100 - 1.000 Endgeräte	1,000 - 5,000	5.000–10.000	10.000–20.000
Prozessoren/-Geschwindigkeit	Zwei Cores/2,4 Ghz oder mehr	Acht Cores/2,4 Ghz oder mehr	Acht Cores/2,4 Ghz oder mehr	Acht Cores/2,4 Ghz oder mehr	8 - 12 Cores/2,4 Ghz oder mehr
Datenträger-geschwindigkeit (in den IOPS)	180 - C: Betriebssystem, SMP	180 - C: Betriebssystem, SMP	180 - C: Betriebssystem 130 - D: SMP	180 - C: Betriebssystem 130 - D: SMP	180 - C: Betriebssystem 130 - D: SMP 130 - E: Speicher
Plattenkapazität	80 GB	80 GB	200 GB	400 GB	600 GB
RAM	4 GB	8 GB	16 GB	16 GB	16 GB (Übergeordnet: 24)
Cache	6MB L2 oder mehr				
Netzwerk	Dual Gigabit - mit Lastverteilung				
Betriebssystem	Windows Server 2008 R2 SP1 x64 Standard Edition				

Hinweis: Ihre Datenträgerkapazitätsanforderungen für Notification Server steigen möglicherweise je nach Ihrer spezifischen Strategie für das Speichern von Bereitstellungsdatenträger-Images, von Patch Management Bulletins und Ihrer Softwarebibliothek.

Die Dienste in Tabelle 4-3, Tabelle 4-4, Tabelle 4-5 können auf einem Site Server kombiniert werden oder, abhängig von Ihrer Umgebung, separat bereitgestellt werden. Häufig werden Paket- und PXE-Dienste auf einem einzelnen Computer installiert.

Hinweis: Site Server ist ein Computer, der eine oder mehrere der Aufgaben-, Paket- oder Netzwerkstartserverdienste (PXE) ausführt. Die Aufgaben-, Paket- und PXE-Dienste können auf einem Site Server kombiniert werden oder, abhängig von Ihrer Umgebung, separat bereitgestellt werden.

Site Server verwenden möglicherweise Windows Workstation oder Windows Server. Für verteilte und große Umgebungen sind möglicherweise zahlreiche Site Server erforderlich, damit die Konfigurationsverwaltungsanforderungen erfüllt werden. Das Auswählen eines Servers oder des Betriebssystem hängt von den gleichzeitigen Sitzungen, die dieser Site Server benötigt, ab. Windows-Workstations sind auf 10 gleichzeitige TCP-Verbindungssitzungen beschränkt, das Windows Server-Betriebssystem unterliegt jedoch nicht denselben Einschränkungen. Für eine Site mit weniger als 100 Endgeräten sind möglicherweise nur 10 Sitzungen erforderlich; für größere Remote-Standorte ist jedoch eventuell ein Windows-Server erforderlich.

Tabelle 4-3 Empfehlungen für physische und virtuelle Hardware für Task Server

Komponente	10 - 100 Endgeräte	100 - 1.000 Endgeräte	1,000 - 5,000	5,000 - 7,500
Betriebssystem	Desktop-Betriebssystem mit den Funktionen "IIS 6.0/7.0" und ".NET Framework 3.5" aktiviert.	Server-Betriebssystem mit den Funktionen "IIS 6.0/7.0" und ".NET Framework 3.5" aktiviert.	Server-Betriebssystem mit den Funktionen "IIS 6.0/7.0" und ".NET Framework 3.5" aktiviert.	Server-Betriebssystem mit den Funktionen "IIS 6.0/7.0" und ".NET Framework 3.5" aktiviert.
Prozessoren	Ein Kern	Zwei Kerne	Vier Kerne	Vier Kerne
Plattenkapazität	5 GB	5 GB	5 GB	5 GB
RAM	2 GB	4 GB	4 GB	8 GB
Cache	6MB L2 oder mehr			

Tabelle 4-4 Empfehlungen für physische und virtuelle Hardware für Package Server

Komponente	10 - 100 Endgeräte	100 - 1.000 Endgeräte	1,000 - 5,000	5,000 - 7,500
Betriebssystem Betriebssystem	Desktop-Betriebssystem	Server-Betriebssystem	Server-Betriebssystem	Server-Betriebssystem
Prozessoren	Ein Kern	Zwei Kerne	Vier Kerne	Vier Kerne

Komponente	10 - 100 Endgeräte	100 - 1.000 Endgeräte	1,000 - 5,000	5,000 - 7,500
Datenträger-geschwindigkeit (in den IOPS)	180 - C: Betriebssystem, SMP	180 - C: Betriebssystem, SMP	180 - C: Betriebssystem 130 - D: SMP	180 - C: Betriebssystem 130 - D: SMP
Plattenkapazität	100 GB - 250 GB	100 GB - 250 GB	100 GB - 250 GB	100 GB - 250 GB
RAM	2 GB	4 GB	4 – 6 GB	4 – 8 GB
Cache	6MB L2 oder mehr			

Tabelle 4-5 Empfehlungen für physische und virtuelle Hardware für Netzwerkstartserver (PXE)

Komponente	10 - 100 Endgeräte	100 - 1.000 Endgeräte	1,000 - 5,000	5,000 - 7,500
Betriebssystem	Desktop-Betriebssystem	Server-Betriebssystem	Server-Betriebssystem	Server-Betriebssystem
Prozessoren	Ein Kern	Zwei Kerne	Vier Kerne	Vier Kerne
Plattenkapazität	100–250 GB	100–250 GB	100–250 GB	100–250 GB
RAM	4 GB	4 GB	4 GB	8 GB

Empfohlene Internet-Gateway-Hardware

Symantec empfiehlt, mindestens zwei Internet-Gateways zur Verfügung zu haben, um Failoveroptionen sowie Lastverteilung bereitzustellen und Kommunikationskontinuität beizubehalten. Jedes Internet-Gateway kann mehrere Notification Server bedienen. Diese Konfiguration wird unterstützt, selbst wenn Notification Server in einer Hierarchiestruktur organisiert werden. Jedes Internet-Gateway unterstützt 1 - 60.000 Endgeräte und 3.000 gleichzeitige Verbindungen.

Siehe "Info zu Cloud-fähiger Verwaltung" auf Seite 31.

Das Ausführen des Internet-Gateways auf einem virtuellen Computer wird nicht empfohlen. Das Ausführen des Internet-Gateways auf virtueller Hardware kann seine Skalierbarkeit um bis zu 40% senken.

Tabelle 4-6 Hardwareempfehlungen für Internet-Gateway

Komponente	Anforderung
Betriebssystem	Windows 2008 R2 SP1 mit der Funktion .NET-Framework 3.5.1 aktiviert
Prozessoren	Dual-Core-CPU
Plattenkapazität	Mindestens 40 GB
RAM	8 GB
Netzwerkadapter	Zwei Netzwerkadapter 1Gbit

Empfohlene Konfiguration für Notification Server mit lokal installierter SQL-Datenbank

Für Umgebungen mit bis zu 5.000 verwalteten Computern ist ein Notification Server mit einer lokal installierten SQL-Datenbank möglicherweise ausreichend. Ein Notification Server mit SQL auf dem gleichen Server wird als eine "On-Box-Installation" von SQL bezeichnet. Symantec empfiehlt das Unterstützen von nicht mehr als 5.000 verwalteten Computern mit On-Box SQL. Sogar mit weniger als 5.000 verwalteten Computern ist die Leistung wahrscheinlich weniger robust als bei einer Off-Box-SQL-Konfiguration. Die Leistungseinbußen sind beim Konsolenreaktionsvermögen und der Inventarerfassung am stärksten wahrnehmbar.

Siehe "Informationen zur Planung Ihrer SQL Server-Konfiguration" auf Seite 39.

Siehe "Info zur Festplattenkonfiguration für SQL Server" auf Seite 41.

Tabelle 4-7 IT Management Suite 7.5 – Empfehlungen für Hardware für Notification Server mit On-Box-SQL

Komponente	Bewertung (1 - 20 Endgeräte)	100 - 1.000 Endgeräte	1.000 - 5.000 Endgeräte	> 5.000 Endgeräte
Prozessoren	Zwei Kerne	Acht Kerne	12 - 16 Kerne	Nicht empfohlen
Festplattendrehzahl (in U/s)	180 - C: OS, SMP 200 - D: SQL	180 - C: OS, SMP 200 - D: SQL	180 - C: OS, SQL App 130 - D: SMP 300 - E: SQL DB 300 - F: Protokolle, TempDB	
Plattenkapazität	80 GB	80 GB	200 GB	
RAM	8 GB	12 GB	20 GB+	

Empfohlene maximale Computeranzahl für IT Management Suite 7.5

Die folgenden Informationen basieren auf der Skalierbarkeitsprüfung für IT Management Suite 7.5 in einer 1 x 6 x 20k-Hierarchiekonfiguration.

Siehe "Empfohlene Hardware für die IT Management Suite 7.5" auf Seite 62.

Siehe "Informationen zur Planung Ihrer Site Server" auf Seite 51.

Tabelle 4-8 Bereiche der empfohlenen, insgesamt eingesetzten Komponenten für IT Management Suite 7.5

Komponenten	Bereich
Verwaltete Computer pro Notification Server.	1 - 20,000
Verwaltete Computer pro Package Server.[1]	1 - 7,500
Verwaltete Computer pro Task Server.[2]	1 – 7.500
Verwaltete Computer pro Netzwerkstartserver.[3]	1 – 7.500
Gleichzeitige PXE-Sitzungen pro Netzwerkstartserver.[3]	200
Gleichzeitige Konsolensitzungen pro Notification Server.	100 (75 Manager + 25 Asset-Manager)
Package Server pro Notification Server.	1 – 600

Komponenten	Bereich
Task Server pro Notification Server.	1 – 600
Netzwerkstartserver pro Notification Server (setzt einen lokalen Task Service und lokalen Package Service voraus).	1 – 300

[1]Diese Anzahl hängt von Paketverwendung und Häufigkeit ab. Die entsprechende Anzahl für eine bestimmte Architektur sollte unter Verwendung der Dateiübertragungsgeschwindigkeiten von Microsoft Windows bestimmt werden, da Package Server im Wesentlichen Dateiserver sind.

[2]Falls Sie Aufgaben übermäßig verwenden möchten, muss diese Zahl aufgrund der Anzahl der zu verarbeitenden Prozesse niedriger sein. In diesem Fall ist die Anzahl der Clientcomputerknoten sekundär.

[3]Deployment Solution hat eine Abhängigkeit mit Task Services. Daher sollte die Anzahl der Clientcomputer der Anzahl der Task Server entsprechen. Jedoch dürfen Deployment-Jobs nicht gleichzeitig auf mehr als 200 Clients pro Task Server gestartet werden. Dieses Szenario kann mehrere Einschränkungen aufweisen:

- Die Festplattengeschwindigkeit des Task Servers, der WinPE und die Images hostet.
- Die Anzahl verfügbarer IP-Adressen in einem bestimmten DHCP-Bereich für neu erkannte Computer.
- Die Größe des Image.

Unterstützte Betriebssysteme für Notification Server und Site Server

Die neueste Version der Symantec Management-Plattform erfordert Windows Server 2008 R2 oder Windows Server 2008 R2 SP1. Jedoch kann die Symantec Management-Plattform Middleware-Komponenten auf Computern hosten, bei denen es sich nicht um Notification Server handelt. Diese Middleware-Komponenten unterstützen einige Betriebssysteme.

Weitere Informationen zur Unterstützung der Symantec IT Management Suite-Plattform finden Sie unter http://www.symantec.com/docs/HOWTO9965.

Der offizielle Name für eine Middleware-Komponente ist "Site Service". Jeder Computer, der als Host für einen Site Service fungiert, wird als Site Server bezeichnet. Beispiele für Site Services sind Package Service und Task Service. Auf einem Site Server kann mindestens ein Site Service installiert sein. Beispiel:

Wenn Sie den Package Server-Site Service ("Package Service") auf einen Computer installieren, wird dieser Computer ein Site Server.

Tabelle 4-9 Unterstützte Betriebssysteme für Notification Server

Typ des Betriebssystems	Unterstütztes Betriebssystem
Microsoft Windows-Server	Windows Server 2008 R2, Windows Server 2008 R2 SP1 und Windows Server 2008 R2 SP2. Windows Server 2008 R2 erfordert einen 64-Bit-Computer. Wenn Sie auf Symantec Management-Plattform 7.1 migrieren, empfiehlt Symantec, dass Sie auf einen neuen Computer migrieren.
Virtueller Host	VMware ESX 4.0 und 5.0 Microsoft Hyper-V Server 2008 R2

Site Server können ein Windows-Workstation-Betriebssystem oder ein Windows-Server-Betriebssystem verwenden. Ein Site Server mit einem installierten Package Service kann auch ein Linux-Server-Betriebssystem verwenden.

Für verteilte und große Umgebungen sind möglicherweise zahlreiche Site Server erforderlich, um Konfigurationsverwaltungsanforderungen zu erfüllen. Notification Server stellt sicher, dass der Site Service nur auf den Computern installiert wird, die den Mindestanforderungen entsprechen. Was Sie als Erstes entscheiden müssen, ist die Anzahl von gleichzeitigen Sitzungen, die Sie benötigen, wenn Sie zwischen einem Server-Betriebssystem und einem Workstation-Betriebssystem auswählen. Eine Windows-Workstation ist auf 10 gleichzeitige TCP-Verbindungen begrenzt, während ein Server-Betriebssystem keine Beschränkungen dieser Art aufweist. Ein Standort mit weniger als 100 Endgeräten benötigt vielleicht nur 10 Sitzungen. Für größere Remote-Sites ist jedoch möglicherweise ein Windows-Server erforderlich.

Tabelle 4-10 Unterstützte Betriebssysteme für Package Service

Typ des Betriebssystems	Unterstütztes Betriebssystem
Microsoft Windows-Desktop	Windows XP SP2 Windows XP SP3 Windows Vista SP1 Windows Vista SP2 Windows 7 Windows 7 SP1 Windows 7 SP2
Microsoft Windows-Server	Windows Server 2003 SP2 Windows Server 2003 R2 SP2 Windows Server 2008 Windows Server 2008 SP2 Windows Server 2008 R2, R2 SP1 und R2 SP2
Linux-Desktops	Red Hat Enterprise Linux 5.7, 5.8, 6.2 und 6.3 Novell SUSE Linux Desktop 10, 11, 11 SP1
Linux-Server	Red Hat Enterprise Linux AS 4 Red Hat Enterprise Linux ES 4 Red Hat Enterprise Linux Server 5,1, 5,2, 5,3, 5,4, 5,5, 5,6 Red Hat Enterprise Linux 6.0 Red Hat Enterprise Linux 6.0 Server Red Hat Enterprise Linux 6.1 Server Novell SUSE Linux Enterprise Server 10 Novell SUSE Linux Enterprise Server 11, 11 SP1

Tabelle 4-11 Unterstützte Betriebssysteme für Task Service

Typ des Betriebssystems	Unterstütztes Betriebssystem
Microsoft Windows-Desktop	Windows XP SP2
	Windows XP SP3
	Windows Vista SP2
	Windows 7
	Windows 7 SP1
Microsoft Windows-Server	Windows Server 2003 SP2
	Windows Server 2003 R2 SP2
	Windows Server 2008
	Windows Server 2008 SP2
	Windows Server 2008 R2, R2 SP1

Siehe "SQL Server-Empfehlungen und Drittanbietersoftware-Anforderungen" auf Seite 75.

Info zu unterstützten SQL Server-Kollatierungen

IT Management Suite 7.5 unterstützt die folgenden SQL Server-Sortierungen:

- Latin1_General_BIN - Veraltetes binäres Format
- Latin1_General_BIN2 - Binäres Format
- Latin1_General_CI_AI - Lateinisches ("normales ") Alphabet, keine Beachtung von Groß/Kleinschreibung, keine Beachtung von Akzenten
- Latin1_General_CI_AS - Lateinisches Alphabet, keine Beachtung von Groß/Kleinschreibung, Beachtung von Akzenten
- Latin1_General_CS_AI - Lateinisches Alphabet, Beachtung von Groß/Kleinschreibung, keine Beachtung von Akzenten
- Latin1_General_CS_AS - Lateinisches Alphabet, Beachtung von Groß/Kleinschreibung, Beachtung von Akzenten

Durch Symantec Installation Manager installierte IIS Rollen-Dienste

Bevor Sie mit der Installation von IT Management Suite beginnen, müssen Sie die Rolle "Web Server (IIS)" auf dem Computer installieren. Wenn die erforderlichen IIS Rollen-Dienste nicht installiert sind, werden Sie auf der Seite "Bereitschaftsprüfung für die Installation" aufgefordert, sie zu installieren. Wenn Sie die Installation bestätigen, kann Symantec Installation Manager diese IIS-Rollendienste automatisch auf dem Server installieren und konfigurieren.

Hinweis: Abgesehen von den IIS-Rollendiensten, die mit dem Webserver installiert werden, müssen Sie eventuell einige zusätzliche IIS-Rollendienste installieren. Diese Rollendienste sind für die Installation von IT Management Suite erforderlich. Symantec Installation Manager identifiziert solche IIS-Rollendienste und fordert Sie auf, sie über die Seite "Bereitschaftsprüfung für die Installation" von Symantec Installation Manager-Installationsassistenten automatisch zu installieren.

Nachfolgend sind die IIS-Rollendienste aufgeführt, die bei der Konfiguration der IIS-Rolle auf dem Computer installiert werden:

- Application Server
  - Unterstützung für Web Server (IIS)
  - Unterstützung des Aktivierungsdienstes für Windows-Prozesse
  - HTTP-Aktivierung
  - Webserver (IIS)
- Webserver
  - Allgemeine HTTP-Funktionen
  - Statischer Inhalt
  - Standarddokument
  - Verzeichnissuche
  - HTTP-Fehler
  - HTTP-Umleitung
- Anwendungsentwicklung
  - ASP.NET
  - .NET-Erweiterbarkeit

- ASP
- ISAPI-Erweiterungen
- ISAPI-Filter

- Systemzustand und Diagnose
  - HTTP-Protokollierung
  - Protokollierungstools
  - Anforderungsüberwachung
- Ablaufverfolgung
- Sicherheit
  - Grundlegende Authentifizierung
  - Windows-Authentifizierung
  - Digest-Authentifizierung
- Clientzertifikatzuordnung-Authentifizierung
- IIS Clientzertifikatzuordnung-Authentifizierung
- URL-Autorisierung
  - Anforderungsfilterung
  - IP- und Domäneneinschränkungen
- Leistung
  - Komprimierung statischer Inhalte
  - Komprimierung dynamischer Inhalte
- Verwaltungstools
  - IIS-Verwaltungskonsole
  - IIS Verwaltungsskripte und Tools
  - Management-Dienst
  - IIS 6-Verwaltungskompatibilität
  - IIS 6-Metabasiskompatibilität
  - IIS 6-WMI-Kompatibilität
  - IIS 6-Skripttools
  - IIS 6-Verwaltungskonsole

SQL Server-Empfehlungen und Drittanbietersoftware-Anforderungen

IT Management Suite 7.5 muss SQL Server entweder On-Box oder Off-Box installiert sein. Die benötigte Version des SQL Servers hängt von der Anzahl der Endgeräte ab, die Sie verwalten.

Tabelle 4-12 Empfehlungen für IT Management Suite 7.5 SQL Server

Beweis des Konzeptes	100 - 1.000 Endgeräte	1.000 bis 5.000 Endgeräte	5.000 - 10.000 Endgeräte	10.000 - 20.000 Endgeräte
Microsoft SQL Server Express 2005 SP4, 2008 SP2 oder höher und 2012.	Microsoft SQL Server 2005 SP2 SP4, 2008 oder höher oder 2012 Standard oder Enterprise. On-Box-SQL wird unterstützt; Off-Box-SQL wird empfohlen.	Microsoft SQL Server 2005 SP2 SP4, 2008 oder höher oder 2012 Standard oder Enterprise. On-Box-SQL wird unterstützt; Off-Box-SQL wird empfohlen.	Microsoft SQL Server 2005 SP2 SP4, 2008 oder höher oder 2012 Standard oder Enterprise. Symantec empfiehlt, dass Sie den SQL Server Off-Box hosten.	Microsoft SQL Server 2005 SP2 SP4, 2008 oder höher oder Enterprise 2012. Symantec empfiehlt, dass Sie den SQL Server Off-Box hosten.

Siehe "Info zu unterstützten SQL Server-Kollatierungen" auf Seite 72.

IT Management Suite 7.5-Lösungen erfordern auch folgende zusätzliche Drittanbietersoftware:

Tabelle 4-13 Für IT Management Suite 7.5 erforderliche Drittanbietersoftware

Software	Zweck
Adobe Flash Player 11	Das Adobe Flash Player-Plugin für Internet Explorer ist für das Ressourcenzuordnungsdiagramm in Asset Management Suite erforderlich.
Adobe Reader	Adobe Reader ist zum Öffnen der Dokumentation erforderlich, die im PDF-Format für ITMS-Lösungen verfügbar ist.
AJAX 1.0	Ajax wird verwendet, um asynchrone Aufrufe zu aktivieren, um eine dynamische Benutzeroberfläche zu ermöglichen. Beispielsweise das Laden von Menüs auf Abruf oder spontane Darstellungen. Ajax ist für viele Elemente der Benutzeroberfläche entscheidend – Menüs, Raster, Verzeichnisstrukturen, Listen, Komponentensteuerelemente usw.
Microsoft Access 2010 OLEDB-Treiber	Data Connector erfordert, dass dieser Treiber in der Lage ist, mit Access- (.mdb) und Excel-Dateien (.xls) zu kommunizieren. Installieren Sie die 64-Bit-Version des Treibers.

Software	Zweck
Microsoft .NET 3.5 SP1 (für Notification Server)	Die Symantec Management-Plattform hängt vom Microsoft .NET Framework ab.
Microsoft .NET 3.5 (für Task Server)	Task Server hängt vom Framework Microsofts .NET ab.
Microsoft Internet Explorer	Microsoft Internet Explorer ist der Browser, der die Symantec Management Console unterstützt. Siehe "Konsole/Browser" auf Seite 136.
Microsoft Silverlight 5	Silverlight ist für die Seite der Ersteinrichtung in der Symantec Management Console erforderlich.
Server Manager-Rollen und Rollendienste	Application Server-Rolle und IISs 6-Verwaltungskompatibilität, ASP und Webserver-Rollendienste. **Hinweis:** Wenn die erforderlichen IIS-Rollendienste nicht installiert sind, werden Sie dazu aufgefordert, sie auf der Seite "Bereitschaftsprüfung für die Installation" zu installieren. Siehe "Durch Symantec Installation Manager installierte IIS Rollen-Dienste" auf Seite 73.
Sun Java Runtime 32-Bit Version 6 oder 7	Java JRE ist für LiveState und Altiris Package Conversion erforderlich. Java JRE ist auch auf jedem Computer erforderlich, der über Remote-Zugriff auf die Symantec Management Console zugreift, wenn die Softwarebibliothek als Paketquelle verwendet wird.

Siehe "Unterstützte Betriebssysteme für Notification Server und Site Server" auf Seite 69.

Kapitel 5

Lösungskommunikationen

In diesem Kapitel werden folgende Themen behandelt:

- Funktionsweise der Aufgaben in Deployment Solution
- Wie Agent-Check-in-Intervalle und Grundinventareinstellungen kommunizieren
- Vorgehensweise bei der agentenbasierten Übermittlung von Inventardaten
- Info zum Konfigurieren von Inventarisierungsrichtlinien- und Aufgabeneinstellungen zur optimalen Ressourcennutzung
- Methoden zum Erfassen von Inventardaten
- Info zur Paketverteilung in einer Hierarchie
- Funktionsweise des Patch Management Solution-Datenaustauschs
- Datenaustausch in der Asset Management Suite
- Auswählen einer Methode für Software Delivery
- Informationen zu Erkennungsregeln
- Erstellen einer Erkennungsregel
- Softwareportal einrichten

Funktionsweise der Aufgaben in Deployment Solution

Deployment Solution lässt Sie Standardverteilungsfunktionen mit der Symantec Management-Plattform integrieren. Sie hilft, die Kosten des Verteilens und des Verwaltens von Servern, Desktops und Notebooks von einer Zentralstelle in Ihrer Umgebung aus zu reduzieren. Die Lösung bietet Betriebssystemverteilung, Konfiguration, Migration von Computerfunktionseigenschaften und

Softwareverteilung über verschiedene Hardwareplattformen und Betriebssystemtypen hinweg.

Wie Agent-Check-in-Intervalle und Grundinventareinstellungen kommunizieren

Einige clientseitige und serverseitige Einstellungen kommunizieren, um beispielsweise zu beeinflussen, wann eine Anwendung auf einigen Endgeräten bereitgestellt wird. Dies erklärt möglicherweise, warum scheinbar nichts passiert, nachdem Sie einen Satz Computer zu einer Richtlinie hinzugefügt haben.

Tabelle 5-1 Reihenfolge für Agent-Server-Kommunikationen

Reihenfolge	Standort	Beschreibung
Eins	Client	Das Grundinventar liefert grundlegende Clientinformationen. Beispielsweise liefert es Informationen zu Agentversion, Sub-Agent, eindeutiger ID usw.
Zwei	Server	Das Update der Ressourcenmitgliedschaft fügt den Computer einem oder mehreren Zielen hinzu. Dies basiert auf dem Grundinventar und anderen Inventarvariablen, die möglicherweise zutreffen, wie zum Beispiel bedingte Parameter, Richtlinien usw.
Drei	Server	Der Zeitplan zur Aktualisierung der Richtlinie verwendet die Mitgliedschaftstabellen, um Richtlinientabellen zu aktualisieren. Wenn ein Benutzer eine Richtlinie speichert, wird sie sofort aktualisiert.
Vier	Client	Die Agentkonfigurationsanfrage wird ausgeführt und findet heraus, welche Richtlinien zutreffen.

Vorgehensweise bei der agentenbasierten Übermittlung von Inventardaten

Inventory Solution ermöglicht die Anzeige ausführlicher Berichte über die Hardware und Software in Ihrer Umgebung. Sie können anhand dieser Informationen Zielcomputer für die Richtlinien und Aufgaben festlegen. Darin enthalten sind vordefinierte Inventarisierungsrichtlinien. Einige vordefinierte Inventarisierungsrichtlinien werden standardmäßig aktiviert. Jedoch können Sie sie jedoch ändern, um spezielle Bedürfnisse zu erfüllen.

Diese Richtlinien umfassen die folgenden Einstellungen:

- Was inventarisiert werden soll.
- Wann die Aufgabe ausgeführt werden soll.
- Auf welchen Computern (Ziele), die Aufgabe ausgeführt werden soll; in der Standardeinstellung werden alle Computer, auf denen das Inventory Solution-Plugin installiert ist, als Zielcomputer festgelegt.
- Optionale erweiterte Einstellungen.

Notification Server sendet die aufgabengestützte Richtlinie für die erste Inventarisierung an den verwalteten Computer. Das Inventory Solution-Plugin führt sofort die erste Inventarisierung aus. Nachdem das Inventory Solution-Plugin über seine Richtlinieneinstellungen verfügt, fährt es mit der Ausführung der Inventarisierungsaufgabe fort. Es führt die Aufgabe entsprechend den Einstellungen und dem Zeitplan aus, die in der Richtlinie definiert sind. Sobald eine Richtlinieneinstellung geändert wird, sendet der Task Server die neuen Einstellungen sofort an das Plugin. Das Inventory Solution-Plugin dann führt sofort eine Inventarisierung durch.

Inventory Solution wird unabhängig von der Konfigurationsanforderung des Symantec Management Agent ausgeführt. Die Vorgänge werden mit Aufgaben und Task Servern durchgeführt. Die Uhrzeit, zu der die Inventarisierung ausgeführt wird, ist auf die Zeitzone der verwalteten Computer bezogen. Es wird nicht die Zeitzone des Notification Server-Computers verwendet.

Sie können Ihre eigenen benutzerdefinierten Zeitpläne in der Richtlinie erstellen, oder Sie können einen der folgenden vordefinierten Zeitpläne verwenden:

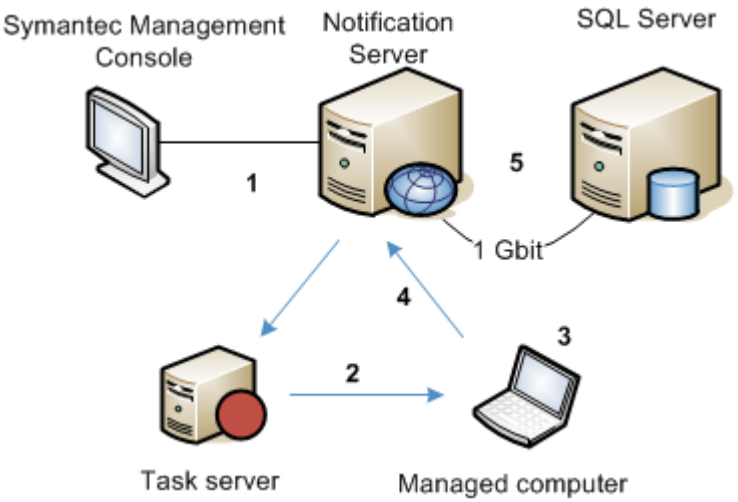
- Täglich. Diese Uhrzeit ist auf täglich 18:00 Uhr festgelegt.
- Wöchentlich. Diese Uhrzeit ist auf jeden Montag 18:00 Uhr festgelegt.
- Monatlich. Diese Uhrzeit ist auf 18:00 Uhr am ersten Montag eines jeden Monats festgelegt.

Wenn das Inventory Solution-Plugin ausgeführt wird, sammelt es Hardware-Inventardaten, Dateiscans, Daten der Microsoft Windows-Systemsteuerung zum Hinzufügen oder Entfernen von Programmen sowie UNIX-, Linux- und Mac-Software-Listen. Das Inventory Solution-Plugin sendet die Daten sofort an den Notification Server. Die Daten werden als Notification Server-Ereignisse (NSEs) zusammengetragen. Notification Server speichert die NSEs in der Configuration Management Database. Die Daten sind dann für die Berichterstellung über die Symantec Management Console verfügbar.

Tabelle 5-2 Schrittfolge für die Übermittlung von Inventardaten

Schrittfolge	Beschreibung
Eins	Vordefinierte Inventarisierungsrichtlinien sind für verwaltete Computer auf Notification Server verfügbar.
Zwei	Nach der ersten Bereitstellung des Inventory-Plugins werden die Inventarisierungsrichtlinien mithilfe der Richtliniendatei des Notification Servers für verwaltete Computer bereitgestellt.
Drei	Standardmäßig wird das Inventory-Plugin so bald wie möglich ausgeführt. Das Inventory-Plugin erfasst dann das Inventar entsprechend dem definierten Zeitplan.
Vier	Nachdem die Inventardaten erfasst worden sind, werden sie standardmäßig sofort an den Notification Server-Computer gesendet.
Fünf	Der Notification Server-Computer speichert die Inventardaten in der CMDB.

Abbildung 5-1 Schrittfolge für die Übermittlung von Inventardaten



Info zum Konfigurieren von Inventarisierungsrichtlinien- und Aufgabeneinstellungen zur optimalen Ressourcennutzung

Mit Inventory Solution können Sie Inventardaten zu Computern, Benutzern, Betriebssystemen und installierten Software-Anwendungen in Ihrer Umgebung erfassen.

Standard-Inventarisierungsrichtlinien- und Aufgabeneinstellungen überbelasten möglicherweise Ihr Netzwerk. Sie können Inventarisierungsrichtlinien- und Aufgabeneinstellungen konfigurieren, um die Auswirkungen auf Ihre Umgebung zu minimieren.

Über die folgenden Empfehlungen justieren Sie die Inventarisierungsleistung, um die Auswirkungen auf Ihrem Umgebung und die Netzwerkarbeitslast zu minimieren:

- Vermeiden Sie die übermäßige Planung von Inventarisierungsaktivitäten.
  Auf der Inventarisierungsrichtlinienseite können Sie festlegen, entsprechend Ihren Notwendigkeiten Inventare zu Hardware und Betriebssystemen, Software, Dateieigenschaften oder Serveranwendungen zu sammeln. Alle diese Typen von Inventardaten müssen nicht gleichzeitig ausgeführt werden.
  Symantec empfiehlt, dass Sie eindeutige Richtlinien und Zeitpläne für verschiedene Arten von Inventarisierung verwenden.
  Beachten Sie: Wenn zu viele Inventarisierungsaufgaben und Richtlinien ausgeführt werden , kann das die Arbeitslast auf dem Notification Server erhöhen.
  Durch das Erhöhen der Häufigkeit einer Inventarisierungsrichtlinie oder -aufgabe, um ein "Online Fenster" zu nutzen, werden überflüssige Daten an den Notification Server gesendet. Die Arbeitslast auf dem Notification Server erhöht sich, da die doppelten Daten verarbeitet und dann verworfen werden müssen. Planen Sie Inventarisierungsrichtlinien oder -aufgaben mit der gewünschten Aktualisierungsrate, damit Symantec Management Agent den Inventarisierungsprozess lokal verwalten kann.
- Verwenden Sie den Typ und die Methode der Inventarisierung, die Ihren aktuellen Notwendigkeiten am besten entsprechen.
  Auf der Inventarisierungsrichtlinienseite können Sie den Inventartyp auswählen und konfigurieren, den Sie sammeln möchten. Sie können auch eine benutzerdefinierte Richtlinie zur Inventarisierung erstellen, um bestimmte Daten zu sammeln. Dies ermöglicht es, den Netzwerkverkehr zu verringern und die Arbeitslast auf dem Notification Server zu reduzieren.
  Siehe "Methoden zum Erfassen von Inventardaten" auf Seite 86.

- Benutzen Sie für wiederkehrende Aktivitäten Richtlinien anstelle von Aufgaben.
  Symantec empfiehlt, für wiederkehrende Inventarisierungsaktivitäten Richtlinien statt Aufgaben zu verwenden.
  Inventarisierungsrichtlinien bieten mehr Optionen und ermöglichen mehr Flexibilität für die laufende reguläre Inventarisierung. Beispiel: Sie können eine Inventarisierungsrichtlinie planen, die auf eine bestimmte Benutzergruppe oder Computergruppe zutrifft, und die Richtlinie wird automatisch auf allen neuen Computern ausgeführt, die Sie der Zielgruppe hinzufügen.
- Überprüfen Sie alle Inventarisierungsaufgaben, bevor Sie sie aktivieren.
  Einige Optionen von Inventarisierungsaufgaben sind standardmäßig aktiviert. Dies kann eine bedeutende Vergrößerung der Datenbank bewirken. Symantec empfiehlt, dass Sie die Aufgabeneinstellungen überprüfen und die Optionen deaktivieren, die nicht für Ihren genauen Zweck notwendig sind.
- Verhindern Sie die übermäßige Verwendung der Richtlinie "Vollständiges Inventar erfassen" und der zugehörigen Inventarisierungsaufgabe.
  Symantec empfiehlt, dass Sie regelmäßig eine volle Inventarisierung ausführen, damit das Inventar immer synchron mit dem Server bleibt. Die Standardempfehlung lautet zwar, wöchentlich ein vollständiges Inventar zu erfassen, Sie können aber die Richtlinieneinstellungen entsprechend Ihren Anforderungen konfigurieren.
  Die zu häufige Ausführung vollständiger Inventarisierungsscans erhöht möglicherweise die Arbeitslast auf dem Notification Server. Um die Last in Ihrer Umgebung zu reduzieren, empfiehlt Symantec längere Abstände zwischen dem Sammeln des vollen Inventars und zwischendurch die Ausführung von Deltainventaren.
  Deltainventarberichte melden nur die Daten, die sich seit dem letzten vollen Inventarisierungsscan geändert haben. Die Ausführung von Deltainventarisierungen hilft die Netzwerkbelastung zu reduzieren.
  Der Vorgang des Sammelns von Deltainventaren ist wie folgt:

Schritt 1	Wenn Sie eine volle Inventarisierungsrichtlinie ausführen, sammelt sie die Informationen über Datenklassen, zeichnet in delta.cache einen Hash für jede Datenklasse auf und schickt diese Informationen an den Notification Server. Sie können die Inventardaten im Ressourcenmanager oder in den Berichten anzeigen.
Schritt 2	Das folgende Deltainventar berechnet ein neues Hash für jede Datenklasse, vergleicht es mit den aktuellen Informationen in delta.cache, aktualisiert delta.cache und schickt dann die geänderten Informationen an den Notification Server.

Schritt 3	Jedes neue Deltainventar aktualisiert die Informationen in delta.cache entsprechend den erkannten Änderungen.
Schritt 4	Wenn Sie ein volles Inventar sammeln, überschreibt es vollständig den vorhandenen delta.cache.

Die Daten in der Configuration Management Database (CMDB) können überholt sein, wenn Sie bedeutende Änderungen an der Umgebung vornehmen, sodass delta.cache auf dem Clientcomputer nicht mehr mit den Informationen in der Datenbank übereinstimmt. Dies tritt möglicherweise auf, wenn Computer zusammengelegt, gelöscht und dann Notification Server wieder hinzugefügt, von einem Notification Server auf einen anderen umgeleitet werden oder eine neue Datenbank verwendet wird.

In diesem Fall empfiehlt Symantec, dass Sie ein volles Inventar ausführen, nachdem Sie die Änderungen vorgenommen haben.

Manchmal können auch die Inventardatendateien beschädigt oder durch den Notification Server nicht verarbeitet worden sein. In diesem Fall müssen Sie einen vollen Inventarisierungsscan ausführen, um die Informationen wieder zu synchronisieren.

- Konfigurieren Sie die Option "Einstellungen für Dateieigenschaftsprüfung".

  Wenn Sie Einstellungen einer Inventarisierungsrichtlinie oder -aufgabe konfigurieren, überprüfen Sie im Dialogfeld "Erweiterte Optionen" die "Einstellungen für Dateieigenschaftsprüfung" auf den folgenden Registerkarten:

Laufwerke	Standardmäßig werden alle lokalen Laufwerke gescannt. Sie können die Laufwerke ausschließen, die Sie nicht scannen müssen.
Ordner	Sie können die Verzeichnisse ausschließen, die Sie nicht scannen müssen.
Dateien	Im Dialogfeld "Dateieinschließungsregeln" empfiehlt Symantec, "Nur Berichtgröße/Dateianzahl" zu aktivieren, wenn Sie keine genauen Informationen über Dateien sammeln müssen. Dies verringert die Netzwerkbelastung.

- Aktivieren Sie die Option "Zugriff auf Netzwerkdateisysteme (Mac/Linux/UNIX)" nur bei Bedarf.

  Das Aktivieren dieser Option im Dialogfeld "Erweiterte Optionen" führt möglicherweise zu überflüssigen Inventardatenberichten.

  Die Scans von Remote-Datenträgern sind standardmäßig deaktiviert, damit nicht zahlreiche Computer redundante Inventardaten senden.

- Konfigurieren Sie die Inventarisierungsscan-Drosselungsoption.

Durch die Drosselung legen Sie den Start des Inventarisierungsscans variabel fest, um die Netzwerkbelastung zu verringern.

Symantec empfiehlt, dass Sie Drosselung in größeren Umgebungen verwenden. Beispiel: Wenn Sie mehrere virtuelle Computer auf einem einzelnen physischen Hostcomputer haben, können sich durch das Ausführen eines Inventarisierungsscans bedeutende Leistungsprobleme ergeben. Durch Drosselung legen Sie die Startzeit des Inventarisierungsscans variabel fest, wodurch auch die Zeit, zu der der Notification Server die Inventarisierungsscanergebnisse erhält, variabel ist. Das Netzwerk und der Notification Server können das Inventar im Laufe der Zeit verarbeiten.

Beispielsweise können Sie den Scandrosselungszeitraum auf 24 Stunden einstellen. Zu der geplanten Zeit startet der Scanvorgang, aber andererseits wechselt er sofort zum Schlafzustand und schließt den Scan später zu einer willkürlichen Zeit innerhalb des angegebenen Zeitraums (in dieses Beispiel 24 Stunden) ab.

Um die Drosselung zu aktivieren, klicken Sie auf einer Inventarrichtlinien- oder Aufgabenseite auf "Erweitert" und im Dialogfeld "Erweiterte Optionen" auf die Registerkarte "Ausführungsoptionen", wo Sie die Option "Inventar-Scan gleichmäßig drosseln über einen Zeitraum von: *X* Stunden" aktivieren.

Beachten Sie: Wenn eine Richtlinie mit dieser Einstellung ausgeführt wird, wird die Ausführung im Aufgabenverlauf angezeigt, selbst wenn sich die Aufgabe während der variablen Ausführung im Schlafzustand befindet.

Hinweis: Diese Funktion ist derzeit nur für Windows verfügbar.

- Konfigurieren Sie die Option "Systemressourcennutzung".

  Diese Option betrifft nur den Dateiscanvorgang und nicht die Sammlung von Daten zu Hardware, Betriebssystem und "Programme hinzufügen/entfernen".

  Die Option "Systemressourcennutzung" ermöglicht es, die Priorität der Inventarisierung festzulegen und folglich die Nutzung des Prozessors und des Datenträgers auf dem Clientcomputer während eines Inventarisierungsscans zu ändern. Um diesen Wert festzulegen, entscheiden Sie, wie schnell Inventardaten gesammelt werden sollen und wie die Inventarisierung die Leistung auf dem Clientcomputer beeinflusst.

  Um diese Option zu konfigurieren, klicken Sie auf einer Inventarisierungsrichtlinien- oder Aufgabeseite auf "Erweitert" und legen sie dann im Dialogfeld "Erweiterte Optionen" auf der Registerkarte "Ausführungsoptionen" den Wert für die "Systemressourcennutzung" entsprechend Ihren Notwendigkeiten fest.

  Wen Sie die Priorität auf einer Windows-Plattform verringern, erfordert der Inventarisierungsvorgang weniger Systemressourcen auf dem Clientcomputer,

aber der Inventarisierungsscan dauert länger. Wenn Sie die Priorität erhöhen, verläuft der Inventarisierungsscan schneller, verbraucht aber auch mehr Ressourcen.
Bei UNIX-, Linux- und Mac-Computern definiert der Wert der "Systemressourcennutzung" die Priorität des Inventarisierungsvorgangs, definiert aber nicht den Prozentsatz der Ressourcennutzung. Auf UNIX-, Linux- und Mac-Plattformen verwenden Computer mehr CPU-Schleifen für Vorgänge mit hoher Priorität und weniger für Vorgänge mit niedriger Priorität. Wenn sich der Computer im Ruhezustand befindet und nur den Inventarisierungsscan ausführt, kann ein Vorgang mit niedriger Priorität die verfügbaren Ressourcen nutzen. CPU-Auslastung wird reduziert, sobald ein anderer Prozess mit höherer Priorität ausgeführt wird.

Hinweis: Auf der Windows-Plattform ist diese Option nur für Dateiscans anwendbar. Auf UNIX-, Linux- und Mac-Plattformen ist diese Option auf den gesamten Prozess des Inventarisierungsscans anwendbar.

- Konfigurieren Sie die Komprimierungseinstellungen.
  Mithilfe von Komprimierung können Sie die Datendateien, die Clientcomputer zum Notification Server schicken, komprimieren. Sie können die minimale Dateigröße, die komprimiert wird, angeben, wenn sie über das Netzwerk gesendet wird. Wenn Sie Komprimierung verwenden wollen, müssen Sie die Balance zwischen Client- und Serverlast und Netzwerknutzung finden.
  Wenn Sie den Komprimierungsschwellenwert auf eine niedrigere Dateigröße festlegen, wird die Arbeitslast sowohl auf dem Clientcomputer als auch dem Notification Server erhöht. Der Clientcomputer muss die Datei komprimieren und der Server muss sie dekomprimieren. Jedoch verringert diese Einstellung die Netzwerklast.
  Wenn Sie den Komprimierungsschwellenwert auf einen höheren Wert festlegen , wird die Arbeitslast auf dem Clientcomputer und dem Server gesenkt. Die Netzwerklast nimmt aber aufgrund der größeren Dateien, die über das Netzwerk gesendet werden, zu.
  Symantec empfiehlt, dass Sie Komprimierung bei kleineren Dateien nur verwenden, wenn Sie eine sehr niedrige Bandbreite haben. Wenn Ihr Notification Server eine Site mit einer hohen Bandbreite versorgt, ist es nicht notwendig, Komprimierung zu verwenden.
  Die Komprimierung wird automatisch für alle Lösungen aktiviert. Um die Komprimierung zu verwenden, konfigurieren Sie die Symantec Management Agent-Einstellungen für den Clientcomputer.

Weitere Informationen erhalten Sie in den Themen über das Konfigurieren der speziellen Agent-Einstellungen im *IT Management Suite 7.5-Administratorhandbuch*
http://www.symantec.com/docs/DOC5330

Methoden zum Erfassen von Inventardaten

Sie können verschiedene Methoden zum Erfassen verschiedener Inventardatentypen verwenden. Jede Methode hat bestimmte Funktionen und Anforderungen.

Tabelle 5-3 Methoden zum Erfassen von Inventardaten

Methode	Beschreibung	Funktionen und Anforderungen
Grundinventarisierung	Grundinventardaten werden automatisch erfasst, wenn Symantec Management Agent auf verwalteten Computern installiert ist. Dies ist eine zentrale Funktion der Symantec Management-Plattform, für die keine zusätzlichen Inventarisierungskomponenten erforderlich sind. Zu den Grundinventardaten gehören: Computername, Domäne, installiertes Betriebssystem, MAC- und IP-Adresse, primäres Benutzerkonto usw. Diese Informationen werden regelmäßig aktualisiert, solange der Symantec Management-Agent auf dem Computer ausgeführt wird.	Folgende Funktionen sind verfügbar: ■ Inventardaten werden automatisch erfasst, wenn der Symantec Management Agent auf dem Clientcomputer installiert ist. Weitere Komponenten oder Schritte sind nicht erforderlich. ■ Inventardaten werden in regelmäßigen Abständen aktualisiert. ■ Sie können diese Methode unter verschiedenen Plattformen verwenden. ■ Sie können diese Methode zum Erfassen von Inventardaten auf verwalteten Windows-Computern in der Cloud-fähigen Verwaltungsumgebung verwenden. Folgende Anforderungen gelten: ■ Zielcomputer müssen unter Verwendung von Symantec Management Agent verwaltet werden. **Hinweis:** Es kann nur eine begrenzte Menge an Grundinventardaten erfasst werden.

Methode	Beschreibung	Funktionen und Anforderungen
Standardinventarisierung auf verwalteten Computern	Inventory-Plugin funktioniert mit Symantec Management Agent und verwendet geplante Richtlinien, um Standardinventardaten zu erfassen, die ausführlicher als Grundinventardaten sind. Standardmäßig werden Standardinventardaten anhand von mehr als 100 vordefinierter Datenklassen erfasst. Zu den Standardinventardaten gehören die folgenden Details zu verwalteten Computern: ■ Hardwarekomponenten, Betriebssystem sowie Benutzerkonten und -gruppen. ■ Software- und virtuelle Softwareschichten. ■ Dateieigenschaften. Ausführlichere Informationen zur Software (z. B. Hersteller, Version, Größe usw.). Wenn das Inventory-Plugin auf verwalteten Computern installiert ist, können Sie alle Inventarisierungsrichtlinien über die Symantec Management Console verwalten. Sie können Inventarisierungsrichtlinien planen, die in regelmäßigen Abständen zu geeigneten Zeiten ausgeführt werden, damit die Inventarisierung die Netzwerkleistung nicht beeinträchtigt. Sie können das Inventory-Plugin kann unter Windows, Linux, UNIX und MacOS verwenden.	Folgende Funktionen sind verfügbar: ■ Erfassen einer breiten Palette an Inventardaten ■ Inventardaten werden automatisch unter Verwendung geplanter Richtlinien und Aufgaben erfasst und aktualisiert. ■ Sie können Richtlinien so konfigurieren, dass nur über die Daten erfasst werden, die sich seit dem letzten vollständigen Inventarisierungsscan geändert haben (Deltainventar). ■ Diese Methode kann untere mehreren Plattformen genutzt werden. ■ Sie können Standardinventardaten auf verwalteten Windows-Computern in der Cloud-fähigen Verwaltungsumgebung sammeln. Folgende Anforderungen gelten: ■ Zielcomputer müssen unter Verwendung von Symantec Management Agent verwaltet werden. ■ Auf Zielcomputern muss das Inventory-Plugin installiert sein. **Hinweis:** Bei Computern, die nicht regelmäßig mit dem Netzwerk verbunden sind, kann das Aktualisieren der Inventardaten schwierig sein.

Methode	Beschreibung	Funktionen und Anforderungen
Standalone-Inventarisierung	Zum Erfassen von Standalone-Inventardaten müssen Sie Standalone-Pakete in der Symantec Management Console erstellen. Dann verteilen Sie die Pakete unter Verwendung von E-Mail, Netzwerkfreigaben, Login-Skripts usw. und führen die Pakete auf den Zielcomputern aus. Mit dieser Methode können Sie Standardinventardaten auf Computern erfassen, die nicht vom Symantec Management Agent verwaltet werden, auf denen das Inventory-Plugin nicht installiert ist und die nicht mit dem Notification Server verbunden sind Sie können ausführliche Informationen zu Hardwarekomponenten, Betriebssystem, lokale Benutzer und -gruppen, Software und virtuelle Softwareschichten erfassen. Sie können diese Methode in der Cloud-fähigen Verwaltungsumgebung nicht verwenden.	Folgende Funktionen sind verfügbar: ■ Erfassen einer breiten Palette an Inventardaten ■ Es werden nur Windows-basierte Computer unterstützt. Folgende Anforderungen gelten: ■ Das Inventarisierungspaket muss extern bereitgestellt werden. ■ Wenn Zielcomputer nicht mit dem Notification Server verbunden sind, müssen die Daten manuell veröffentlicht werden. **Hinweis:** Die Inventardaten werden nicht zentral verwaltet und sind möglicherweise nicht aktuell.

Methode	Beschreibung	Funktionen und Anforderungen
Benutzerdefinierte Inventarisierung	Zum Erfassen benutzerdefinierter Inventardaten müssen Sie das Inventory-Plugin auf den verwalteten Computern installieren. Mithilfe dieser Methode können Sie zusätzliche Daten erfassen, die über die vordefinierten Datenklassen in Inventory Solution hinausgehen. Sie können zusätzlich benutzerdefinierte Inventardatenklassen spezifisch für Ihre Umgebung erstellen. Anschließend können Sie die benutzerdefinierten Skripts ausführen, die die benutzerdefinierten Inventardatenklassen erfassen.	Folgende Funktionen sind verfügbar: ■ Sie können die Datenklassen hinzufügen, die in Ihrer Umgebung eindeutig und nicht standardmäßig enthalten sind. ■ Sie können eine Beispielskriptaufgabe verwenden, um eine benutzerdefinierte Inventarisierungs-Skriptaufgabe zu erstellen oder zu konfigurieren. ■ Diese Methode wird unter verschiedenen Plattformen unterstützt. ■ Sie können diese Methode zum Erfassen von Inventardaten auf verwalteten Windows-Computern in der Cloud-fähigen Verwaltungsumgebung verwenden. Folgende Anforderungen gelten: ■ Zielcomputer müssen unter Verwendung von Symantec Management Agent verwaltet werden. ■ Auf Zielcomputern muss das Inventory-Plugin installiert sein. ■ Sie müssen benutzerdefinierte Inventardatenklassen erstellen und diese in die benutzerdefinierten Skripts aufnehmen. ■ Sie müssen die benutzerdefinierten Skripts erstellen und ausführen, die die benutzerdefinierten Inventardatenklassen erfassen.

Methode	Beschreibung	Funktionen und Anforderungen
Softwarenutzungsverfolgung und Application Metering	Zum Einsatz von Softwarenutzungsverfolgung und Application Metering müssen Sie Inventory-Plugin und Application Metering-Plugin auf den verwalteten Computern installieren. Sie können die Anwendungsnutzungsdaten und die Übersicht über die überwachten Anwendungen erfassen. Sie können die folgenden Aufgaben auf verwalteten Computern ausführen: ■ Sie können die Nutzung der verwalteten Software auf Produkt-, Komponenten- und Versionsebene durch Aktivieren der Softwarenutzungsverfolgung überwachen. Diese Aufgabe ist für die meisten Softwareprodukte geeignet. ■ Sie können die Nutzung und Verfügbarkeit von Anwendungen überwachen und steuern, indem Sie vor- oder benutzerdefinierte Application Metering-Richtlinien ausführen. Symantec empfiehlt, diese Aufgabe nur zum Überwachen von Start-, Stopp- und Verweigerungsereignissen für Anwendungen auf Dateiebene zu verwenden. ■ Sie können das Ausführen mehrerer Anwendungen verweigern, indem Sie die vordefinierte Richtlinie "Anwendungen in der Blackliste" konfigurieren oder benutzerdefinierte Application Metering-Richtlinien ausführen.	Folgende Funktionen sind verfügbar: ■ Sie können die Verfügbarkeit von Anwendungen steuern. Sie können das Ausführen von Anwendungen verweigern. Sie können auch festlegen, dass Ereignismeldungen an den Notification Server gesendet werden, wenn ein Benutzer versucht, eine gesperrte Anwendung auszuführen. ■ Mit der Funktion "Softwarenutzungsverfolgung" können Sie auf Produktebene prüfen, ob eine Anwendung installiert ist und wie oft sie genutzt wird. Diese Funktion erleichtert die Verwaltung von Anwendungslizenzen. ■ Sie können diese Methode zum Erfassen von Inventardaten auf verwalteten Windows-Computern in der Cloud-fähigen Verwaltungsumgebung verwenden. Folgende Anforderungen gelten: ■ Zielcomputer müssen unter Verwendung von Symantec Management Agent verwaltet werden. ■ Auf Zielcomputern müssen das Inventory- und Application Metering-Plugin installiert sein. ■ Es werden nur Windows-basierte Computer unterstützt. **Hinweis:** Diese Methode wird auf Windows-Servern nicht unterstützt.

Methode	Beschreibung	Funktionen und Anforderungen
Basisinventarisierung	Zum Erfassen von Basisinventardaten müssen Sie das Inventory-Plugin auf den verwalteten Computern installieren. Mithilfe dieser Methode können Sie Daten zu Dateien und Registrierungseinstellungen auf Computern erfassen. Sie können eine Basis erzeugen, die die Dateien oder die Registrierungseinstellungen eines Computers identifiziert. Zu einem späteren Zeitpunkt können Sie die Compliance-Scans auf verwalteten Computern ausführen, bei denen die aktuellen Dateien bzw. Registrierungsschlüssel mit denen der Basis verglichen werden. Die Unterschiede zwischen dem Basis-Scan und dem Compliance-Scan werden an die CMDB gemeldet.	Folgende Funktionen sind verfügbar: ■ Sie können die Dateien und die Registrierungen verfolgen, die von den Unternehmensstandards abweichen. ■ Sie können die Genauigkeit von Rollouts und Upgrades überprüfen. ■ Systemadministratoren bzw. Helpdesk-Personal können automatisch benachrichtigt werden, wenn ein Computer nicht den Anforderungen entspricht. ■ Sie können eine Übersicht auf Compliance-Ebene des Computers und Berichte zu den Änderungen in den Dateien anzeigen. Folgende Anforderungen gelten: ■ Zielcomputer müssen unter Verwendung von Symantec Management Agent verwaltet werden. ■ Auf Zielcomputern muss das Inventory-Plugin installiert sein. ■ Es werden nur Windows-basierte Computer unterstützt. **Hinweis:** Sie können diese Methode in der Cloud-fähigen Verwaltungsumgebung nicht verwenden.

Methode	Beschreibung	Funktionen und Anforderungen
Inventory für Netzwerkgeräte	Inventory für Netzwerkgeräte erfasst Inventardaten auf im Netzwerk erkannten Geräten. Diese Inventardaten werden auf Geräten erfasst, die nicht über den Symantec Management Agent verwaltet werden. Da kein Verwaltungs-Agent erforderlich ist, gilt diese Inventarisierung als "ohne Agent". Auf folgenden Gerätetypen können Inventarisierungsdaten erfasst werden: ■ Cluster ■ Computer ■ Computer: Virtueller Computer ■ Infrastrukturgerät ■ IP-Telefon ■ KVM-Gerät ■ Netzwerkverbundener Speicher ■ Netzwerksicherungsgerät ■ Netzwerkdrucker ■ Out-of-Band-Management-Gerät ■ Out-of-Band-Management-Gerät: Gehäuseverwaltungs-Controller ■ Physisches Rack ■ Physisches Gehäuse ■ Physischer Schacht	Folgende Funktionen sind verfügbar: ■ Bei der Inventarisierung ohne Agent werden auf den Geräten, die bereits erkannt wurden und als Ressourcen in der Configuration Management Database (CMDB) der Symantec Management-Plattform vorhanden sind, Inventardaten erfasst. Folgende Anforderungen gelten: ■ Bevor Sie Inventardaten auf Netzwerkgeräten erfassen, müssen Sie die Daten über die SNMP-fähigen Geräte im Netzwerk erfassen. ■ Bevor Sie Inventardaten auf Netzwerkgeräten erfassen, muss im Verbindungsprofil der Aufgabe "Network Discovery" die Option "SNMP" aktiviert sein.

Info zur Paketverteilung in einer Hierarchie

Der Vorgang der Paketverteilung in einer Hierarchie umfasst mehrere Phasen. Die Hauptfaktoren, die den Prozess beeinflussen, sind die Paketgröße und die Bandbreite.

Die Zeit, die jede Phase für die Fertigstellung benötigt, hängt von den Einstellungen ab, die Sie angeben. Die folgende Tabelle beschreibt den Vorgang der Paketverteilung bei den Standardeinstellungen.

Tabelle 5-4 Vorgang der Paketverteilung in einer Hierarchie

Phase	Vorgangsbeschreibung	Geschätzte Zeit
1	Sie erstellen ein Paket auf dem übergeordneten Notification Server.	Die erforderliche Zeit zum Erstellen eines Pakets hängt von der Größe des Pakets ab.

Phase	Vorgangsbeschreibung	Geschätzte Zeit
2	Der übergeordnete Package Server, der dem übergeordneten Notification Server zugewiesen ist, fordert Richtlinien an.	Der Vorgang dauert möglicherweise bis zu 75 Minuten, falls Sie Standard-Replikationseinstellungen verwenden (1 Stunde-Richtlinien-Anfragezeitüberschreitung plus 15 Minuten für Delta-Updatezeitplan).
3	Der übergeordnete Package Server lädt das Paket von einem übergeordneten lokalen Verzeichnis des Notification Servers oder von einer alternativen Netzwerkressource herunter.	Die Zeit, die für das Herunterladen des Pakets erforderlich ist, hängt von der Paketgröße und der Bandbreite ab.
4	Die nächste Replikation (vollständig oder differenziell) vom übergeordneter Notification Server auf den untergeordneter Notification Server findet statt. Die Paketverteilungsrichtlinie und alle Informationen über das Paket werden repliziert.	Die Replikation nimmt (bei Standard-Replikationseinstellungen) möglicherweise bis zu 24 Stunden in Anspruch, plus den Zeitraum, der benötigt wird, um Daten zu replizieren. Wenn Sie das Paket nach dem der Start der Replikation erstellen, wird dieses Paket erst bei der Replikation am nächsten Tag repliziert.
5	Der untergeordnete Package Server, der dem untergeordneten Notification Server zugewiesen ist, fordert Richtlinien an.	Der Vorgang dauert möglicherweise bis zu 75 Minuten, falls Sie Standard-Replikationseinstellungen verwenden (1 Stunde-Richtlinien-Anfragezeitüberschreitung plus 15 Minuten für Delta-Updatezeitplan).

Phase	Vorgangsbeschreibung	Geschätzte Zeit
6	Der untergeordnete Package Server fordert das Paketverzeichnis vom untergeordneter Notification Server an. Der untergeordnete Notification Server leitet den untergeordneten Package Server zum übergeordneter Notification Server um, der ihn dann zum übergeordneten Package Server umleitet.	Die Paketverzeichnisanfrage und die Serverumleitung passieren fast sofort.
7	Der untergeordnete Package Server lädt das Paket vom übergeordneten Package Server herunter.	Die Zeit, die für den Download erforderlich ist, hängt von der Paketgröße und der Bandbreite ab.

Phase	Vorgangsbeschreibung	Geschätzte Zeit
8	Der untergeordnete Package Server schickt seine Codebasen (die Daten über den Speicherort des Pakets) an den untergeordneten Notification Server. Diese Informationen werden durch andere Package Server verwendet, die das Paketverzeichnis anfordern. Sofern nicht alle vorherigen Schritte abgeschlossen wurden, erhält der untergeordnete Package Server eine leere Liste der Paketverzeichnisse und versucht das Herunterladen des Pakets erneut.	Wenn der untergeordnete Package Server ein Paket nicht herunterladen kann, wiederholt er den Versuch alle 3*2n Minuten, bis er das 24-stündige Limit erreicht. Danach wiederholt er den Versuch alle 24 Stunden. Der Server beendet die erneuten Versuche, das Paket herunterzuladen, wenn das Paket gelöscht wird oder nicht mehr anwendbar ist. **Hinweis:** Um Zeit zu sparen, können Sie eine eigenständige Replikationsregel erstellen, die auf dem übergeordneten Package Server häufiger läuft, und nur Paketobjekte und ihre Zuordnungen (Programm- und Befehlszeilenobjekte) repliziert.

Funktionsweise des Patch Management Solution-Datenaustauschs

Patch Management Solution inventarisiert die verwalteten Computer, um die erforderlichen Betriebssystem- und Software-Updates (Patches) zu bestimmen. Die Anwendung lädt dann die erforderlichen Patches herunter und stellt Assistenten zur Verfügung, mit denen Sie die Patches verteilen. Mithilfe der Lösung können Sie einen Patch-Updatezeitplan einrichten, um sicherzustellen, dass verwaltete Computer immer die aktuellen Sicherheitsupdates der Anbieter erhalten. Verwaltete Computer werden dann fortlaufend geschützt.

Sie können Patch Management Solution planen, um kritische Sicherheitsbulletins in die CMDB automatisch herunterzuladen. Symantec empfiehlt, diesen Zeitplan für Windows-Computer auf täglich und für Linux-Computer auf wöchentlich festzulegen. Nach diesem Zeitplan werden nicht die Patch-Installationsdateien, sondern nur die in den Sicherheitsbulletins darüber enthaltenen Informationen heruntergeladen. Dieser Download wird Software-Update-Katalog genannt. Der

erste Software-Update-Katalogimport auf einer neuen Plattform kann einige Stunden dauern. Jedoch dauern nachfolgende Importe in der Regel weniger als eine Stunde an, weil bei jedem Import nur die geänderten Dateien heruntergeladen werden, die häufig nur einige MB umfassen. Wenn Sie mehrere Sprachen aktivieren, dann vergrößert sich die Anzahl von Sicherheitsbulletins, die herunterzuladen sind, die Größe der Downloads und der zum Herunterladen erforderliche Zeitraum. Sie können Software-Update-Katalogaktualisierungen anpassen, indem Sie Ausnahmen für die Software erstellen, die Sie nicht patchen möchten. Sie können benutzerdefinierte Zeitpläne für den Download erstellen.

Standardmäßig kontaktiert das Software-Update-Plugin alle vier Stunden den Notification Server, um zu prüfen, ob Patches vorliegen. Wenn neue Sicherheitsbulletins durch den Software-Update-Katalog der CMDB hinzugefügt werden, prüft das Software-Update-Plugin, ob sie anzuwenden sind. Es prüft auch, ob die Updates bereits installiert worden sind. Es sendet die Ergebnisse der Prüfung an den Notification Server-Computer. Die Daten sind für die Berichterstellung zur Richtlinieneinhaltung verfügbar.

Nachdem der Software-Update-Katalogimport abgeschlossen worden ist, können Sie auswählen, welche Sicherheitsbulletins auf Notification Server implementiert werden sollen. Diese Staging-Prozesse veranlassen den Download der Patch-Installationsdateien in einen Ordner auf dem Notification Server-Computer.

Nachdem der Download der Patches abgeschlossen ist, können Sie die Patch-Verteilungsrichtlinie erstellen und aktivieren. Wenn Sie mehrere Package Server verwenden, legen Ihre Standortverwaltungseinstellungen für die Paketverteilung fest, wie die Patch-Installationsdateien auf die Package Server verteilt werden.

Die Richtlinie wird erst angewendet, nachdem sich der Symantec Management-Agent angemeldet hat. Standardmäßig kontaktiert der Symantec Management-Agent den Notification Server-Computer stündlich und fordert Konfigurationsupdates an. Sie können jedoch einen anderen Zeitplan verwenden.

Der Notification Server-Computer sendet die Patchverteilungsrichtlinie an den Symantec Management-Agent. Der Notification Server-Computer gibt den Standort des Package Servers dem Symantec Management-Agent bekannt. Der Symantec Management-Agent stellt eine Verbindung zum Package Server her und lädt die Patches herunter.

Nachdem die Patches heruntergeladen worden sind, wartet die Installation mit der Ausführung auf das nächste planmäßige Wartungsfenster. Sie wartet, sofern Sie nicht festgelegt haben, dass die Wartungsfenster für Zero-Day-Exploits ignoriert werden sollen.

Dann werden folgende Schritte ausgeführt:

- Es wird überprüft, ob die Patches heruntergeladen worden sind.

- Die Patches werden installiert, und der Computer wird neu gestartet.
  Sie können die Neustarteinstellungen konfigurieren, damit der Server nicht unmittelbar nach der Aktualisierung mit Patches neu gestartet wird. Für Clientcomputer kann kein Neustartfenster festgelegt werden, damit die Benutzer den Neustart aufschieben können.
- Es wird eine Risikoanalyse ausgeführt.
  Wenn kein Neustart durchgeführt wurde, wird der Computer möglicherweise in Berichten als angreifbar angezeigt.

Nachdem der Patch-Prozess abgeschlossen worden ist, sendet das Software-Update-Plugin die aktualisierte Risikoanalyse an den Notification Server und speichert sie in der CMDB. Sie können die Compliance-Berichte verwenden, um Informationen zu Sicherheitslücken auf der Symantec Management Console anzuzeigen.

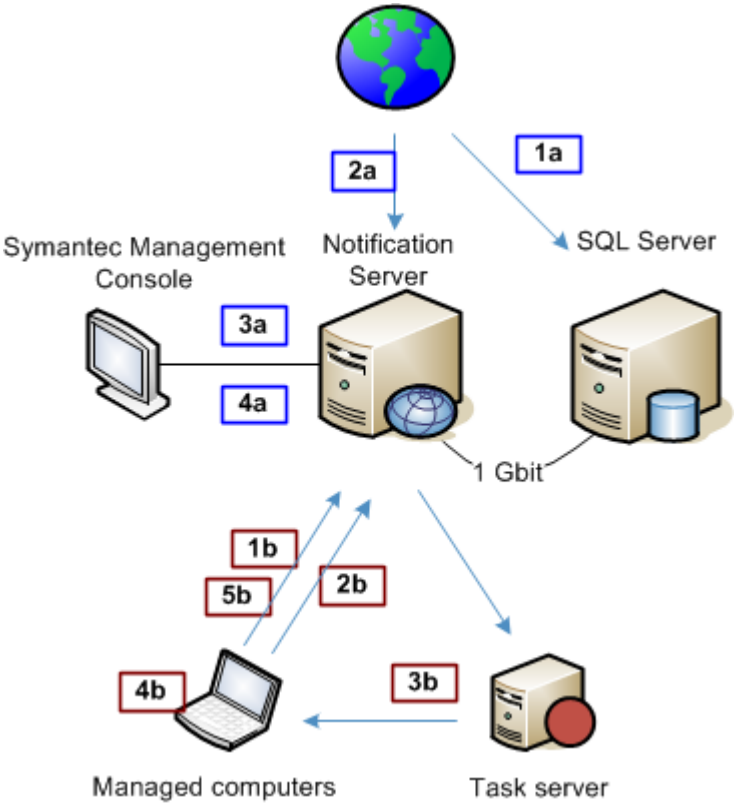
Da der Patch-Prozess mehrere Abhängigkeiten aufweist, ist die Reihenfolge der Vorgänge wichtig. Das Software-Update-Plugin dient zum Ermitteln von Sicherheitsrisiken. Symantec Management Agent führt das Software-Update durch. Sie können jeweils einen anderen Update-Zeitplan haben. Der größere Zeitplan definiert das Zeitfenster, in dem Patches an die verwalteten Computern geliefert werden können. Das Wartungsfenster definiert, wann die Patches installiert werden. Compliance-Berichte zeigen erst einen Erfolg an, nachdem diese Schritte abgeschlossen worden sind.

Tabelle 5-5 Schrittfolge für den Patch-Datenaustausch

Schrittfolge	Beschreibung
Eins (a)	Auf Notification Server wird automatisch ein Import ausgeführt und Sicherheitsbulletins werden in die CMDB geladen.
Zwei (a)	Sie wählen die Patches im Sicherheitsbulletin aus, und die Patches werden in einem lokalen Ordner auf dem Notification Server-Computer installiert.
Drei (a)	Sie erstellen eine Patch-Verteilungsrichtlinie und geben darin die Patches an, die heruntergeladen wurden.
Vier (a)	Nachdem die Agents die Ausführung abgeschlossen haben, führen Sie einen Compliance-Bericht aus, um den Patch-Status zu prüfen.
Eins (b)	Das Patch-Plugin meldet sich standardmäßig alle vier Stunden an. Es verwendet die neuesten Patch-Management-Importdaten und führt eine Überprüfung auf Sicherheitslücken aus. Diese Überprüfung ist vom Abschluss des Patch-Management-Imports abhängig.

Schrittfolge	Beschreibung
Zwei (b)	Symantec Management Agent meldet sich an und erhält die neuesten Patch-Richtlinien und den Speicherort der Patches.
Drei (b)	Symantec Management Agent lädt die Patch-Pakete vom Notification Server-Computer oder von seinem zugewiesenen Package Server herunter.
Vier (b)	Während des nächsten Wartungszeitraums installiert Symantec Management-Agent die Patches. Nach der Installation werden die Einstellungen für den Computerneustart ausgeführt.
Fünf (b)	Nachdem das Paket installiert worden ist, wird erneut eine Sicherheitslückenanalyse ausgeführt, und die Informationen werden an den Notification Server-Computer geschickt.

Abbildung 5-2 Schrittfolge für den Patch-Datenaustausch



Datenaustausch in der Asset Management Suite

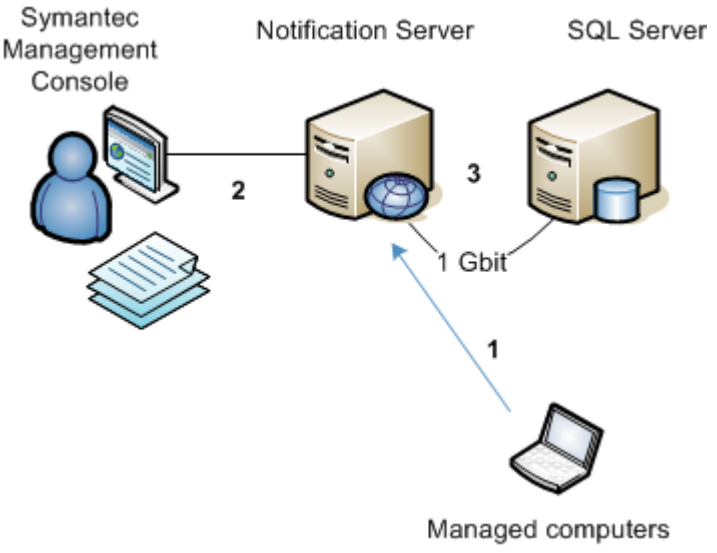
Asset Management Suite bietet eine Management-Konsole, eine Datenbankumgebung und eine Reihe von Lösungen, mit denen Sie Assets und asset-spezifische Informationen verfolgen können.

Die Suite umfasst Asset Management Solution, Barcode Solution und CMDB Solution. Sie ist besonders auf die Verfolgung IT-spezifischer Assets, wie z.B. Computer und Software, ausgelegt. Sie können damit auch andere von Typen Assets verfolgen, z. B. Büromaschinen oder Fahrzeuge.

Tabelle 5-6 Schrittfolge für den Datenaustausch in der Asset Management Suite

Schrittfolge	Beschreibung
Eins	Asset Management Solution verlässt sich darauf, dass Inventory Solution Daten über verwaltete Computer sammelt und liefert.
Zwei	Der Administrator fügt nicht-verwaltete Assets unter Verwendung der Symantec Management Console hinzu.
Drei	Die in der CMDB gespeicherten Daten sind für die Berichterstellung verfügbar, und Administratoren können Berichte zum Erstellen von Verwaltungsrichtlinien verwenden.

Abbildung 5-3 Schrittfolge für den Datenaustausch in der Asset Management Suite



Auswählen einer Methode für Software Delivery

Sie können Software auf einen oder mehrere verwaltete Computer verteilen, indem Sie eine Softwareverwaltungsaufgabe bzw. -richtlinie erstellen und ausführen. Die Methode zum Erstellen der Aufgabe bzw. Richtlinie hängt von Ihren Verteilungsanforderungen ab.

Verwenden Sie zur schnellen Verteilung einer einzelnen Softwareressource die aufgabenbasierte Methode "Schnellverteilung", um die zu verteilende Software, die durchzuführende Aktion und die Computer für die Verteilung anzugeben. Wegen ihrer Einfachheit ist die Schnellverteilung eine ideale Methode für Nicht-Administratoren (z. B. Helpdeskpersonal), Software sicher und genau zu verteilen.

Außerdem können Sie die aufgabenbasierte Paketverteilung verwenden, um ein Paket zu verteilen, das nicht einer Softwareressource zugewiesen ist.

Um eine erweiterte Softwareverteilung durchzuführen, können Sie eine intelligente richtlinienbasierte Methode zur kontrollierten Softwareverteilung verwenden. Diese Verteilungsmethode unterstützt wiederkehrende Zeitpläne, Softwareabhängigkeiten, Softwareersetzung, Sequenzierung, Virtualisierung und andere komplizierte Verteilungsszenarien.

Tabelle 5-7 Methoden für das Verteilen von Software

Anforderung	Verteilungsmethode	Beschreibung
Ausführen einer Schnellverteilung einer einzelnen Softwareressource	Schnellverteilung	Sie können die aufgabengestützte Schnellverteilungsmethode verwenden, um die zu verteilende Software, die auszuführende Aktion und die Computer anzugeben, auf denen die Software verteilt werden soll. Die Schnellverteilung nutzt die Standardaufgabeneinstellungen, die Sie ggf. ändern können. Wegen ihrer Einfachheit ist die Schnellverteilung eine ideale Methode für Nicht-Administratoren (z. B. Helpdeskpersonal), Software sicher und genau zu verteilen. Die Software, die Sie auf diese Weise verteilen, muss im Softwarekatalog als verteilbare Softwareressource definiert sein.

Anforderung	Verteilungsmethode	Beschreibung
Ausführen einer oder mehrerer der folgenden erweiterten Verteilungsaktionen: ■ Verteilung anhand eines wiederkehrenden Zeitplans ■ Installieren auf einen bekannten Zustand und Sicherstellen, dass der Zustand beibehalten wird ■ Gleichzeitiges Installieren der Software und der anderen Software, von der sie abhängt ■ Installieren einer Softwareressource, die eine andere Software ersetzt ■ Sequenzielles Installieren mehrerer Anwendungen und Aufgaben ■ (Nur Windows) Installieren von Software in eine virtuelle Softwareschicht. ■ Ausführen einer beliebigen Clientaufgabe zu einem beliebigen Zeitpunkt der Verteilung Eine Clientaufgabe ist eine Aufgabe, die im Notification Server definiert ist und auf einem Clientcomputer ausgeführt werden soll.	Kontrollierte Softwareverteilung	Die kontrollierte Softwareverteilung ist eine richtliniengestützte Verteilungsmethode, mit der Sie erweiterte Verteilungsanforderungen erfüllen können. Eine einzelne kontrollierten Softwareverteilungsrichtlinie kann mehrere Verteilaktionen ausführen. Die Software, die Sie auf diese Weise verteilen, muss im Softwarekatalog als verteilbare Softwareressource definiert sein. Die kontrollierte Softwareverteilung nutzt die im Softwarekatalog enthaltenen Softwareressourceninformationen und Logikelemente. Beispielsweise nutzt die kontrollierte Softwareverteilung die Abhängigkeiten, das Paket und die Erkennungsregel der Softwareressource.
Verteilen von Software als Reaktion auf eine direkte Anfrage eines Benutzers	Softwareportal	(Nur Windows und Mac) Mit dem Softwareportal können Benutzer um Software bitten und auf auf diese Anforderungen reagieren. Ist der Benutzer berechtigt, die Software zu installieren, wird die Installation ohne Eingreifen des Administrators durchgeführt. Andernfalls muss der Administrator nur die Anfragen genehmigen und die Software verteilen, die nicht im Softwarekatalog ist.
Verteilen von Paketen, die nicht mit einer Softwareressource verknüpft sind	Paketverteilung	Die Paketverteilung ist eine aufgabengestützte Verteilungsmethode. Mit ihr können Sie ein beliebiges Paket unabhängig davon verteilen, ob es mit einer Softwareressource verknüpft ist.

Anforderung	Verteilungsmethode	Beschreibung
Verteilen von Software mit einer Richtlinie, die aus Software Delivery Solution 6.x. migriert wurde.	Legacy-Software Delivery	Wenn Sie von Notification Server 6.x auf Symantec Management-Plattform 7 aktualisieren, können Sie Ihre 6.x-Software Delivery-Aufgaben auf Legacy-Verteilungsrichtlinien migrieren. Sie können diese Richtlinien weiterhin verwenden, wie sie sind. Sie können ihre Pakete auch Softwareressourcen zuweisen, um ein 6.x-Softwarepaket mit Schnellverteilung oder kontrollierter Softwareverteilung zu verteilen.
(Nur Windows) Installieren von Software in eine neue virtuelle Softwareschicht auf einem Clientcomputer.	Softwarevirtualisierungsaufgabe Schnellverteilung Paketverteilung	Importiert eine VSA- oder eine XPF-Datei auf einen verwalteten Clientcomputer und erstellt eine neue virtuelle Softwareschicht.
(Nur Windows) Virtualisieren einer Anwendung und Installieren in eine neue virtuelle Softwareschicht auf einem Clientcomputer	Kontrollierte Softwareverteilung	Sie können neue virtuelle Softwareschichten erstellen und verwalten oder vorhandene Schichten auf Clientcomputern verwalten. Mit einer verwalteten Software Delivery-Richtlinie können Sie komplexe Schichtenverwaltungsaufgaben durchführen.

Informationen zu Erkennungsregeln

Anhand von Erkennungsregeln kann festgestellt werden kann, ob bestimmte Software auf einem Clientcomputer installiert ist. Außerdem dienen Erkennungsregeln dazu, dass softwarebezogene Vorgänge die Softwareressourcen genau identifizieren können.

Im Folgenden finden Sie Beispiele für die Verwendung von Erkennungsregeln:

- Bei der Software Management Solution wird durch eine Richtlinie für kontrollierte Verteilung die Software nur installiert, wenn die zugehörige Erkennungsprüfung feststellt, dass die Software noch nicht installiert ist. Dadurch wird verhindert, dass die Software auf den Computern erneut installiert wird, auf denen sie bereits installiert ist.
- Bei Inventory Solution verwendet die Richtlinie für zielgerichtete Softwareinventarisierung ebenfalls eine Erkennungsregel, um festzustellen, ob eine bestimmte Softwareressource auf Clientcomputern installiert ist. Die Richtlinie gibt dann die Computer aus, die die Software enthalten.

Eine Erkennungsregel kann nach Informationen (Dateizuordnungen, MSI-Produktcode, Verknüpfungen und Registrierungseinträgen) suchen. Wenn sie jene Dateien findet, wird angenommen, dass die Softwareressource installiert wurde. Eine Erkennungsregel stellt sicher, dass durch Software Discovery eine EXE-basierte installierte Softwareressource festgestellt und zur Liste "Neu erkannte Software" hinzugefügt werden kann.

Regeln sind mit Softwareressourcen verbunden. Eine Regel wird nicht Weise verwendet, wenn sie mit keiner Softwareressource verbunden ist. Wenn Sie jedoch eine Softwareressource löschen, werden keine Regeln gelöscht, die Sie mit dieser Softwareressource erstellt und verbunden haben. Die Regeln verbleiben in der Datenbank.

Bewährte Methoden zum Erstellen von Regeln:

- Im Allgemeinen sollten Erkennungsregeln spezifisch genug sein, um eine bestimmte Version einer Softwareressource von anderen Versionen unterscheiden zu können. Aber die Regeln sollten nicht so spezifisch sein, dass die Erkennung fehlschlägt. Wenn Sie beispielsweise Dateiausdrücke erstellen, sollten Sie keine bestimmte Dateiversion verwenden. Geben Sie stattdessen verschiedene Versionen an.
- Versuchen Sie, Regeln so einzurichten, dass sie Dateipfade finden, indem sie sie aus der Registrierung extrahieren, anstatt in einem bestimmten Pfad zu suchen. Auf diese Weise können Sie Regeln einrichten, indem Sie den Ausdruckstyp "Registrierungsschlüssel/Dateipfad zu Dateiversion" verwenden. Dieser Ausdruckstyp liest den Dateipfad aus der Registrierung und vergleicht ihn mit einem Versionsbereich.
- Mit Hilfe der Softwareerkennung lassen sich Dateiressourcen zwar einer Softwareressource hinzufügen, nicht jedoch einer Erkennungsregel. Erstellen Sie mit diesen Dateiressourcen eine Erkennungsregel oder aktualisieren Sie eine bestehende Erkennungsregel.

Erstellen einer Erkennungsregel

Anhand von Erkennungsregeln kann festgestellt werden kann, ob bestimmte Software auf einem Clientcomputer installiert ist. Außerdem dienen Erkennungsregeln dazu, dass softwarebezogene Vorgänge die Softwareressourcen genau identifizieren können. Die Verwendung der Erkennungsregel verhindert die erneute Installation von Software auf Computern, auf denen die Software bereits vorhanden ist.

So erstellen Sie eine Erkennungsregel

1. Klicken Sie in der Symantec Management Console im Menü "Verwaltung" auf "Softwarekatalog".
2. Führen Sie im Fenster "Softwarekatalog" einen der folgenden Schritte aus:
   - Wählen Sie bei einer undefinierten Software-Ressource diese im Teilfenster "Neu erkannte bzw. nicht definierte Software" aus und klicken Sie dann auf das Symbol "Bearbeiten".
   - Suchen Sie bei einer definierten Software-Ressource das Softwareprodukt, mit dem die Software-Ressource verknüpft ist, im Teilbereich "Verwaltete Softwareprodukte" oder "Nicht verwaltete Software". Klicken Sie anschließend auf das Softwareprodukt und öffnen Sie im Dialogfeld "Softwareprodukt" die entsprechende Softwareressource in der Liste auf der Registerkarte "Inventar identifizieren".
3. Klicken Sie auf der Seite "Softwareressource" auf die Registerkarte "Regeln".
4. Klicken Sie auf der Registerkarte "Regeln" neben der Dropdown-Liste für Erkennung auf das Symbol "Neue Erkennungsregel hinzufügen".
5. Geben Sie im Dialogfeld "Regel erstellen" im Feld "Name" einen Namen als Beschreibung der Regel ein.
6. Um einen Operator in der Symbolleiste zu hinzuzufügen, klicken auf das Symbol "Neuen Regelausdruck hinzufügen", dann auf "Operatoren" und wählen dann einen Operator aus.

   Das Symbol "Neuen Regelausdruck hinzufügen" ist nur aktiviert, wenn ein Operator im linken Teilfenster ausgewählt wird.
7. Um einen neuen Regelausdruck in der Symbolleiste zu erstellen, klicken auf das Symbol "Neuen Regelausdruck hinzufügen", dann auf eine der folgenden Optionen und wählen den Ausdruck aus:
   - Standardregel
     Standardregeln sind statisch und können nur Standardregelausdrücke enthalten.
   - Smart-Regel
     Einige Smart-Regeln sind dynamisch und alle Smart-Regeln können Smart- und Standardregelausdrücke enthalten.
8. Bearbeiten Sie die erforderlichen Felder, um den Ausdruck hinzuzufügen.
9. Klicken Sie auf "OK".
10. Fügen Sie Ausdrücke hinzu, bis die Regel vollständig ist.

11 Klicken Sie auf der Seite "Softwareressource" auf "Änderungen speichern".

12 Schließen Sie die Softwareressource.

Softwareportal einrichten

Das Softwareportal ermöglicht, dass Benutzer Anfragen senden und Software durch eine webbasierte Schnittstelle mit weniger oder keiner Administratorbeteiligung installieren. Dieser Selbstbedienungsansatz zur Software Delivery reduziert Helpdeskanrufe und vereinfacht den Prozess des Anforderns und des Verteilens der Software. Weil das Softwareportal vordefinierte Informations- und -verteilungseinstellungen verwendet, kann es die meisten Verteilungen automatisieren, die aus den Softwareanfragen resultieren.

Bevor das Softwareportal verwendet werden kann, muss das Software Management Solution-Plugin auf den Computern installiert sein, auf denen Sie das Softwareportal implementieren.

Tabelle 5-8 Verfahren zum Einrichten des Softwareportals

Schritt	Aktion	Beschreibung
Schritt 1	Konfigurieren Sie Sicherheitsrollen für die Administratoren und Manager, die das Softwareportal verwenden müssen.	Die Sicherheitseinstellungen stellen die Berechtigungen zur Verfügung, um Softwareanfragen der Benutzer zu verwalten und zu genehmigen. Die folgenden Typen von Benutzern kommunizieren mit dem Softwareportal: ■ Spftware-Portal-Administrator ■ Softwarekatalog-Administrator ■ Manager ■ Benutzer
Schritt 2	Konfigurieren des Softwareportals	Die Softwareportaleinstellungen passen das Verhalten und die Darstellung des Portals an. Sie können diese Einstellungen jederzeit nach der Implementierung des Softwareportals ändern.
Schritt 3	Installieren Sie das Softwareportal-Plugin auf den Clientcomputern.	(Nur Windows) Führen Sie diesen Schritt jedes Mal durch, wenn Sie das Softwareportal auf den Clientcomputern installieren, auf denen es noch nicht vorhanden ist. Das Softwareportal-Plugin stellt über den Clientcomputer einen Zugriff auf die Softwareportal-Web-Anwendung zur Verfügung. Das Plugin installiert auch Verknüpfungen zur Softwareportal-Schnittstelle auf dem Clientcomputer.

Schritt	Aktion	Beschreibung
Schritt 4	Definieren Sie die Software, die im Softwareportal erscheint.	Bevor ein Benutzer Software vom Softwareportal anfordern kann, müssen Sie die Software definieren, die der Benutzer anfordern kann. Führen Sie diesen Schritt immer durch, wenn Sie dem Notification Server Benutzer oder Softwareressourcen hinzufügen. Beispiele: ■ Wenn die Finanzabteilung einen neuen Angestellten einstellt, fügen Sie diesen Angestellten den Softwareressourcen hinzu, die für Mitarbeiter in der Finanzabteilung erforderlich sind. ■ Wenn ein Administrator eine neue Softwareressource zum Softwarekatalog hinzufügt, fügen sie auch die Benutzer hinzu, die für Softwareanfragen berechtigt sind. Sie können Software im Softwareportal folgenderweise definieren: ■ Veröffentlichen Sie eine Softwareressource, um eine Schnellverteilung einer einzelnen Softwareressource mit einer Mindestkonfiguration durchzuführen. ■ Veröffentlichen Sie eine verwaltete Software Delivery-Richtlinie, um auf komplexe Verteilungsanforderungen zu reagieren.
Schritt 5	Anweisen von Benutzern und Managern, ihre Profile zu konfigurieren	Jede Person, die das Softwareportal auf einem Clientcomputer verwendet, muss ihr Benutzerprofil konfigurieren, bevor Anfragen erstellt und verarbeitet werden können. Ein Benutzerprofil enthält die Informationen, die den Benutzer im Softwareportal identifiziert. Die Benutzer des Managertyps müssen ebenfalls die Benutzer angeben, deren Softwareanforderungen verarbeitet werden sollen. Außerdem können die Benutzer ihre Voreinstellungen für den Empfang von E-Mail-Nachrichten zu Anforderungen angeben.

Kapitel 6

Empfehlungen zum Feinabstimmen und Optimieren der Leistung

In diesem Kapitel werden folgende Themen behandelt:

- Info zum Bestimmen, ob Sie eine Leistungsoptimierung benötigen
- Leistungsfaktoren der Symantec Management-Plattform
- Informationen zur Leistungsoptimierung der Notification Server-Ereignisverarbeitung
- Info zu vordefinierten Inventarisierungsrichtlinien
- Planen von Ressourcen-Mitgliedschaftsaktualisierungen
- Informationen über die Leistungsoptimierung des Symantec Management Agents
- Empfohlene Konfigurationseinstellungen basierend auf verwalteten Endgeräten
- Informationen zur Leistungsverbesserung der Symantec Management-Plattform-Konsole

Info zum Bestimmen, ob Sie eine Leistungsoptimierung benötigen

Wenn Sie bereits über ein System verfügen, fallen Ihnen eventuell einige Symptome auf, die anzeigen, dass Sie eine Leistungsoptimierung benötigen. Sie können die Leistungsoptimierung auch präventiv einsetzen und so verhindern, dass diese Symptome überhaupt erst auftreten.

Hier sind einige Indikatoren für die Leistungsoptimierung aufgeführt:

- Zufällige Serverfehler
- Zeitüberschreitungen des Servers
- Zeitüberschreitungen bei Abfragen
- Langsame Ausführung
- Auffüllen von Warteschlangen
- Caching-Warnungen im Protokoll
- Übermäßige Deadlock-Wiederholungen im Protokoll
- Zähler für wichtige Leistungsaspekte (Festplatte, Wartestatus)

Andere Symptome können weniger offensichtlich sein. Hier sind einige Beispiele: Leistungsindikatoren für Gebucht-Anforderungen des IIS-Servers sowie Probleme mit der Festplattenlatenz erfordern unter Umständen eine genauere Überprüfung. In einigen Fällen kann es so scheinen, als ob der Server nur um Ruhezustand befindet. Beispielsweise kann es zu starke IIS-Kommunikation kommen, die abgewiesen wird. Zum Beispiel keine CPU, keine Festplatte, kein SQL und niedriges Netzwerk.

Siehe "Leistungsfaktoren der Symantec Management-Plattform" auf Seite 108.

Leistungsfaktoren der Symantec Management-Plattform

Viele Faktoren wirken sich auf die Leistung Ihrer Infrastruktur aus.

Der Durchsatz des SQL Servers ist ein primärer Aspekt für die Symantec Management-Plattformleistung. Die Konfiguration des SQL Server und seiner Hardware beeinflusst die Gesamtleistung. Die meisten Entscheidungen, die sich auf die Leistung auswirken, hängen mit der Auswahl hinsichtlich der Architektur zusammen. Beispielsweise ist die Leistung des SQL Server höher, wenn dieser auf einem anderen Server als Notification Server installiert ist. Dies wird als "Off Box"-Installation bezeichnet. Dabei wird die Arbeit der Datenverarbeitung ausgelagert und Ressourcen werden für die Notification Server-Verarbeitung freigegeben. Eine andere Entscheidung, die die SQL-Leistung beeinflusst, ist Datenträger-E/A.

Im Folgenden sehen Sie einige der gemeinsamen Elemente, die sich auf die Leistung auswirken:

Siehe "Informationen zur Leistungsoptimierung der Notification Server-Ereignisverarbeitung" auf Seite 109.

Siehe "Informationen über die Leistungsoptimierung des Symantec Management Agents" auf Seite 113.

Siehe "Informationen zur Leistungsverbesserung der Symantec Management-Plattform-Konsole" auf Seite 116.

Informationen zur Leistungsoptimierung der Notification Server-Ereignisverarbeitung

Ein Notification Server-Ereignis (NSE) ist der Standardmechanismus, über den Notification Server Daten erhält. Die NSE-Verarbeitung wirkt sich direkt auf die Leistung auf dem Notification Server-Computer aus. Die direkteste Methode zur Beeinflussung der Verarbeitung von NSEs besteht darin, den Datenträger und die Häufigkeit Ihrer Inventarerfassungseinstellungen anzupassen. Sie können die Verarbeitung von NSEs auch beeinflussen, indem Sie die Zeitpläne für Ressourcenmitgliedschafts-Updates anpassen.

Die folgenden Zeitpläne beeinflussen die Verarbeitung von NSEs:

- Vollständiges Inventar erfassen
  Mit dem vollständigen Inventar können Sie Daten über verwaltete Computer erfassen. Es schließt Daten über Hardware, Betriebssystem, installierte Software und Dateieigenschaften ein. Diese Daten werden an den Notification Server im NSE-Format gesendet. Vollständiges Inventar kann ressourcenintensiv sein. Der Standardzeitplan führt eine vollständige Inventarisierung einmal pro Monat aus. Die optimale Vorgehensweise besteht darin, ein vollständiges Inventar einmal im Monat während der Zeiten zu erfassen, in denen die Produktion stillsteht. Sie sollten das vollständige Inventar mehr als einmal wöchentlich ausführen, sogar in kleinen Umgebungen.
  Das benutzerdefinierte Inventar kann häufiger und leistungsfähiger ausgeführt werden als das vollständige Inventar. Bei der benutzerdefinierten Inventarisierung können Sie sehr spezifische Datenpunkte sammeln.
  Siehe "Info zu vordefinierten Inventarisierungsrichtlinien" auf Seite 110.
- Delta-Inventar erfassen
  Die Delta-Inventarisierung und die vollständige Inventarisierung weisen eine ähnliche Ressourcennutzung auf verwalteten Computern auf. Ein Delta-Inventar enthält alle Informationen, die seit der vorherigen Inventarisierung hinzugefügt, entfernt oder geändert wurden. Die Delta-Inventardatei ist kleiner als die Datei des vollständigen Inventars. Die Erfassung des Delta-Inventars kann täglich oder wöchentlich ausgeführt werden. Sie können die Leistung der Symantec Management Console-Benutzeroberfläche steigern, indem Sie das Delta-Inventar außerhalb von Produktionszeiten erfassen. Wir empfehlen, dass Sie das Delta-Inventar wöchentlich anstatt jeden Tag für Umgebungen mit mehr als

10.000 Clients pro Notification Server ausführen. Für Umgebungen mit weniger als 10.000 Clients kann ein täglicher Delta-Inventarzeitplan empfehlenswert sein.

Delta-Inventar kann entfernte Software nicht nachverfolgen. Nur das vollständige Inventar verfolgt entfernte Software nach.

Siehe "Info zu vordefinierten Inventarisierungsrichtlinien" auf Seite 110.

- Ressourcen-Mitgliedschaftsaktualisierungen.

  Die Ressourcenmitgliedschafts-Aktualisierungszeitpläne legen fest, wie genau und aktuell Ihre Ressourcenfilter, Organisationsgruppen und Ressourcenziele sind. Notification Server hat drei Zeitpläne für Ressourcenmitgliedschafts-Updates: Zeitplan für vollständiges Update, Zeitplan für Delta-Updates, Zeitplan für Richtlinienupdates. Je häufiger die Ressourcenmitgliedschafs-Updates ausgeführt werden, desto geringer ist die Zugriffsverzögerung bei Updates oder Reparatur. Wenn jedoch Ressourcenmitgliedschaftsaktualisierungen ausgeführt werden, muss Notification Server die Daten in CMDB lesen und analysieren. Wenn Notification Server Ressourcenmitgliedschaftsaktualisierungen ausführt, werden Datenverarbeitungsressourcen verbraucht. Ein Beispiel, wie der Ressourcenmitgliedschafts-Aktualisierungszeitplan Ihre Alltagsverwendung beeinflussen kann, besteht im Zuweisen der Software vom Softwareportal. Benutzer, die Software vom Softwareportal anfordern, müssen warten, bis die Delta-Ressourcenmitgliedschaftsaktualisierungen abgeschlossen sind.

  Siehe "Planen von Ressourcen-Mitgliedschaftsaktualisierungen" auf Seite 111.

Siehe "Leistungsfaktoren der Symantec Management-Plattform" auf Seite 108.

Info zu vordefinierten Inventarisierungsrichtlinien

Sie können vordefinierte Inventarisierungsrichtlinien verwenden, um schnell Inventardaten zu erfassen. Sie können vordefinierte Richtlinien entsprechend Ihrer Anforderungen konfigurieren. Wenn Sie eine vordefinierte Richtlinie konfigurieren möchten, empfiehlt Symantec, sie zu duplizieren und dann die Kopie zu konfigurieren.

Tabelle 6-1 Vordefinierte Inventarisierungsrichtlinien

Richtlinie	Standardmäßig aktiviert?	Standard-Zeitplan	Standard-Ziel	Hinweise
Vollständiges Serverinventar erfassen (Inventory Pack für Server erforderlich)	Ja	Wöchentlich, jeden Montag um 18.00 Uhr	Alle Computer mit installiertem Inventory Pack for Servers-Plugin	Diese Aufgabe ist nur dann verfügbar, wenn Inventory Pack for Servers installiert ist. Obwohl diese Richtlinie standardmäßig aktiviert ist, müssen Sie das Inventory Pack for Servers-Plugin auf Zielcomputern installieren, bevor Inventardaten erfasst werden.
Delta-Serverinventar erfassen (Inventory Pack für Server erforderlich)	Nein	Wöchentlich, jeden Montag um 18.00 Uhr	Alle Computer mit installiertem Inventory Pack for Servers-Plugin	Standardmäßig erfasst diese Richtlinie nur die Server-Software-Inventardaten, die sich seit der letzten vollständigen Serverinventarisierung geändert haben.

Planen von Ressourcen-Mitgliedschaftsaktualisierungen

Sie können alle Ihre Ressourcenfilter, Organisationsgruppen und Ressourcenziele auf dem aktuellen Stand halten, indem Sie die entsprechenden Zeitpläne für die Filteraktualisierung konfigurieren. Anhand dieser Zeitpläne können Sie Filter, Organisationsgruppen und Ziele aktualisieren, die Sie in geeigneten Intervallen benötigen. Diese Zeitpläne unterstützen Sie beim Verwalten der Verarbeitungslast für Notification Server.

Vordefinierte Zeitpläne für die Ressourcen-Mitgliedschaftsaktualisierung werden in Symantec Management-Plattform bereitgestellt. Diese Zeitpläne sind für die meiste Zwecke geeignet, und Sie sollten sie nicht ändern müssen. Wenn sich jedoch die Anforderungen Ihrer Organisation ändern, können Sie die notwendigen Änderungen vornehmen.

Tabelle 6-2 Zeitpläne für die Ressourcen-Mitgliedschaftsaktualisierung

Zeitplan	Beschreibung
Delta-Aktualisierungs-zeitplan	Aktualisiert die Mitgliedschaft von Folgendem: ■ Filter, deren Mitgliedschaft seit der letzten Aktualisierung geändert wurde. ■ Alle dynamischen Organisationsgruppen. ■ Alle ungültigen Ziele. Ein Ziel kann durch die folgenden Ereignisse ungültig werden: ■ Seine Definition wird gespeichert. ■ Die Mitgliedschaft eines Filters, der es verwendet, ändert sich. ■ Die Mitgliedschaft einer Organisationsgruppe, die es verwendet, ändert sich. ■ Die Sicherheit ändert sich, die auf eine Organisationsgruppe, die es verwendet, angewendet wird. Standardmäßig wird dieser Zeitplan alle fünf Minuten ausgeführt.
Aktualisierungszeitplan fertig stellen	Dadurch wird die Mitgliedschaft aller Filter, Organisationsgruppen und Ziele unabhängig von Inventarstatus oder von Änderungen an Richtlinien komplett neu erstellt. Die vollständige Aktualisierung hat unter Umständen eine beträchtliche Last für Notification Server zur Folge und sollte dementsprechend geplant werden. Standardmäßig wird dieser Zeitplan einmal täglich ausgeführt.
Richtlinien-aktualisierungs-zeitplan	Aktualisiert die Mitgliedschaft der Filter, die eine Richtlinie verwendet, wenn sich die Richtlinie seit der letzten Aktualisierung geändert hat. Durch diesen Zeitplan wird sichergestellt, dass beim Aktualisieren oder Erstellen einer Richtlinie alle Filter, die in den neuen oder geänderten Richtlinienzielen enthalten sind, automatisch aktualisiert werden. Standardmäßig wird dieser Zeitplan alle fünf Minuten ausgeführt.

So konfigurieren Sie Zeitpläne für Ressourcen-Mitgliedschaftsaktualisierungen

1. Klicken Sie in Symantec Management Console im Menü "Einstellungen" auf "Notification Server > Aktualisierung der Ressourcenmitgliedschaft".
2. Konfigurieren Sie auf der Seite "Aktualisierung der Ressourcenmitgliedschaft" die Aktualisierungszeitpläne, die Sie verwenden möchten.

3 Wenn Sie einen Aktualisierungszeitplan sofort ausführen möchten, klicken Sie im entsprechenden Fenster auf "Ausführen".

Beispielsweise können Sie sicherstellen, dass alle Änderungen an Ihren Filtern sofort angewendet werden, statt bis zur geplanten Aktualisierung zu warten.

4 Klicken Sie auf "OK".

Informationen über die Leistungsoptimierung des Symantec Management Agents

Symantec Management-Agent bietet drei allgemeine Einstellungen, die sich auf die Leistung Ihres Notification Server-Computers und die Netzwerkbandbreitennutzung auswirken können. Sie können auf diese Einstellungen in Symantec Management Console, auf der Seite Einstellungen > Agents/Plugin-Einstellungen > Spezifische Einstellungen zugreifen.

Siehe "Leistungsfaktoren der Symantec Management-Plattform" auf Seite 108.

Der Agent bietet die folgenden allgemeinen Einstellungen:

- Neue Konfiguration herunterladen.
  Diese Einstellung ist das Zeitintervall, in dem Symantec Management Agent neue Richtlinieninformationen vom Notification Server anfordert. Änderungen zur Einstellung beeinflussen die Leistung Ihres Notification Server-Computers.
  Der Symantec Management Agent kommuniziert regelmäßig mit Notification Server, um zu ermitteln, ob Arbeit ansteht. Dieses Intervall ist die primäre Einstellung für Agentkommunikationszeitrahmen und legt fest, wie schnell Arbeit den verwalteten Computern bereitgestellt werden kann. Je häufiger Ihre verwalteten Computer eine neue Konfiguration anfordern, desto höher ist die Geamtlast, die auf den Ressourcen des Notification Server-Computers und dem Netzwerk lastet. Die Konfigurationsanforderung selbst erhöht die Last auf dem Notification Server-Computer nicht. Vielmehr ist es so, dass die Arbeit, die der Notification Server-Computer leisten muss, um auf jede Anforderung zu reagieren, die Last erhöht. Sie können das Anforderungsintervall ändern, um die Gesamtanzahl der Anforderungen und die Gesamtlast des generierten Netzwerkverkehrs anzupassen.
  Das Standardintervall für Anforderungen zum Herunterladen neuer Konfigurationseinstellungen beträgt eine Stunde. Eine typische Anforderung generiert ungefähr 3 kbit Netzwerkverkehr.
  Beispielsweise stellen 5.000 verwaltete Computer täglich insgesamt 120.000 Anforderungen an Notification Server, was sich auf ungefähr 360.000 kbit Netzwerkverkehr beläuft. Indem Sie jedoch alle zwei Stunden einstellen, reduzieren Sie die Anzahl von Anforderungen auf 60.000. Sie reduzieren

außerdem den Netzwerkverkehr auf 180.000 kbit. Dieser Zeitplan halbiert den Netzwerkverkehr auf dem Notification Server-Computer; jedoch verdoppelt er auch die Zeit zwischen den Updates auf die verwalteten Computer.
Verwenden Sie die folgenden Richtlinien, um den entsprechenden Wert für das Symantec Management Agent-Konfigurations-Update-Intervall festzulegen:

Anzahl verwalteter Computer	Intervall für Agent-Konfigurationsupdates
< 1.000 Endgeräte	Jede Stunde
1.000 bis 5.000 Endgeräte	Jede Stunde
5.000 bis 10.000 Endgeräte	Alle zwei Stunden
10.000 bis 15.000 Endgeräte	Alle drei Stunden
15.000 bis 20.000 Endgeräte	Alle vier Stunden

- Grundinventar übertragen alle.
  Diese Einstellung ist das Intervall, in dem der Symantec Management Agent Grundinventar an den Notification Server sendet. Notification Server verwendet die Informationen, um jeden verwalteten Computer eindeutig zu identifizieren. Grundinventar enthält Informationen, wie zum Beispiel eine Liste des installierten Agents/der Plugins und der TCP/IP-Adresse. Das Standardintervall lädt Grundinventar einmal täglich hoch. Die Größe eines typischen Grundinventar-Updates liegt zwischen 20 kbit und 25 kbit.
- Ereignisse komprimieren, die größer sind als.
  Diese Einstellung legt fest, zu welcher Größe Notification Server-Ereignissen komprimiert werden, bevor der Agent sie an den Notification Server sendet. Wenn Sie diesen Wert erhöhen, reduzieren Sie die Bandbreitenlast; jedoch erhöhen Sie die Nutzung von CPU-Ressourcen auf verwalteten Computern und Notification Server. Diese Zunahme tritt auf, weil die Computer die Daten komprimieren und dekomprimieren müssen, bevor sie verarbeitet werden können. Die empfohlene Mindestgröße für das Komprimieren eines Notification Server-Ereignisses beträgt 200 KB. Diese Einstellung optimiert die Bandbreitennutzung mit der CPU-Auslastung.
  Sie können zum Beispiel einen niedrigen Wert für die Ereignisse einstellen, die von mobilen Computern gesendet werden. Sie können einen höheren Wert für Ereignisse auf LAN-Computern mit guter Verbindung festlegen.

Empfohlene Konfigurationseinstellungen basierend auf verwalteten Endgeräten

In diesem Abschnitt finden Sie Empfehlungen für allgemeine Konfigurationseinstellungen für den Agent-, Inventar-, Ressourcenmitgliedschafts- und den Task Service-Aktualisierungszeitplan, die die Leistung von IT Management Suite beeinflussen können.

Siehe "Leistungsfaktoren der Symantec Management-Plattform" auf Seite 108.

Tabelle 6-3 Konfigurationseinstellungen basierend auf der Anzahl verwalteter Endgeräte

Einstellung	< 1.000 Endgeräte	1.000 - 5.000 Endgeräte	5.000 - 10.000 Endgeräte	10.000 - 15.000 Endgeräte	> 15.000 Endgeräte
Agent-Konfigurationszeitplan	Jede Stunde	Jede Stunde	Alle zwei Stunden	Alle drei Stunden	Alle vier Stunden
Vollständiger Inventarerfassungszeitplan	Monatlich	Monatlich	Monatlich	Monatlich	Monatlich
Delta-Inventarerfassungszeitplan	Wöchentlich	Wöchentlich	Wöchentlich	Wöchentlich	Wöchentlich
Vollständiger Ressourcenmitgliedschafts-Aktualisierungszeitplan	Täglich	Täglich	Täglich	Täglich	Täglich
Aktualisierungszeitplan der Delta-Ressourcenmitgliedschaft	Alle 15 Minuten	Alle 20 Minuten	Alle 30 Minuten	Alle 45 Minuten	Jede Stunde
Task Service-Aktualisierungszeitplan	Alle 5 Minuten	Alle 5 Minuten	Alle 15 Minuten	Alle 15 Minuten	Alle 15 Minuten

Sie können die folgenden Anpassungen auch durchführen, um die Leistung zu verbessern:

- Reduzieren Sie für Aufgaben u. Richtlinien die Zielgruppenadressierung und Zeitpläne.
- Optimieren Sie die Berichte, die Sie häufig ausführen so, dass Sie die Ressourcenansichten der niedrigsten Ebene in der Ressourcentyphierarchie abfragen.
- Optimieren Sie alle benutzerdefinierten Filter und fragen Sie die Ressourcenansichten der niedrigsten Ebene in der Ressourcentyphierarchie ab.

Informationen zur Leistungsverbesserung der Symantec Management-Plattform-Konsole

In großen Umgebungen empfiehlt Symantec die Verwendung der Funktion "Automatische Ausführung des Berichts unterdrücken". Wenn in NS Configurator die Funktion "Automatische Ausführung des Berichts unterdrücken" aktiviert ist und Sie einen Bericht öffnen, wird der Bericht nicht unmittelbar ausgeführt. Um die Ergebnisse des Berichts anzuzeigen, klicken Sie auf "Aktualisieren". Beachten Sie, dass die Funktion "Automatische Ausführung des Berichts unterdrücken" standardmäßig deaktiviert ist. Sie können die Funktion aktivieren, indem Sie in "NS Configurator" die Optionen "Core-Einstellungen > Benutzeroberfläche > Bericht > Automatische Ausführung des Berichts unterdrücken" aufrufen.

In großen Umgebungen empfiehlt Symantec auch das Konfigurieren der Einstellungen für erweiterte Ansicht. Sie können bestimmte Suchfelder so konfigurieren, dass Sie Ihre Ergebnisse bei der Eingabe der Parameter sehen können. Sie können dieselben Suchfelder auch so konfigurieren, dass Sie Ihre Ergebnisse erst nach dem Drücken der **Eingabetaste** sehen.

Sie können die erweiterten Ansichten so konfigurieren, dass sie IME (Input Method Editor) verwenden, damit Sie Doppelbyte-Zeichen in diesen Ansichten eingeben können. Sie können auch die Anzahl von Computern und Softwareprodukten konfigurieren, die in der Ergebnisliste angezeigt werden.

Um die Einstellungen der erweiterten Ansicht zu konfigurieren, klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Konsole > Erweiterte Ansichten".

Kapitel 7

Umgebungen mit mehreren Notification Servers

In diesem Kapitel werden folgende Themen behandelt:

- Replikationstypen der Symantec Management-Plattform
- Info zur Hierarchiereplikation
- Einsatzmöglichkeiten der Hierarchiereplikation
- Info zur Hierarchietopologie
- So funktionieren Site Server in einer Hierarchie
- Überlegungen zur Implementierung der Hierarchiereplikation für Software Management Solution
- Überlegungen zur Implementierung der Hierarchiereplikation für Patch Management Solution
- Einschränkungen der Hierarchiereplikation
- Implementieren der Notification Server-Hierarchie
- Info zu Peer-zu-Peer-Replikation und Replikationsregeln
- Informationen zur MultiCMDB-Berichtserstellung mit IT Analytics

Replikationstypen der Symantec Management-Plattform

Symantec Management-Plattform verwendet die folgende Replikationstypen:

Hierarchiereplikation.	Kopiert die Informationen zwischen mehreren Notification Server-Computern. Sie definiert, welche Elemente repliziert werden, die Richtung, in die jeder Elementtyp übertragen wird, und wann die Replikation auf jedem Server in der Plattform auftritt. Sie können die Replikation nutzen, um Richtlinien, Aufgaben und Berichterstellungsinformationen auf andere Notification Server-Computer zu kopieren.
Peer-zu-Peer-Replikation	Erfordert, dass Sie die zu replizierenden Elemente und die Richtung definieren, in die sie repliziert werden sollen. Sie müssen die Regeln sehr sorgfältig konfigurieren, weil es in der Peer-Replikation keine automatische Konfliktprävention gibt. Sie können Hierarchiereplikation und Peer-Replikation innerhalb einer Symantec Management-Plattform-Umgebung gleichzeitig verwenden. In früheren Versionen wurde diese Methode der Replikation "Inventarweiterleitung" genannt.

Info zur Hierarchiereplikation

Mit Hierarchiereplikation können Sie von einem Computer des übergeordneter Notification Servers globale Richtlinien erstellen und steuern. Die Hierarchie stellt einige globale Verwaltungsfunktionen zur Verfügung, wahrt jedoch die Autonomie des untergeordneten Notification Server. Richtlinien, Aufträge und Aufgaben werden auf jedem untergeordneten Notification Server-Computer verwaltet, während globale Richtlinien zentral vom übergeordneten Notification Server-Computer aus verwaltet werden.

Der Großteil der täglichen Verwaltungsaufgaben sollte auf jedem Notification Server-Computer unter Verwendung der webbasierten Konsole durchgeführt werden . Sie können jedoch einige Richtlinien, die für alle Endgeräte gelten, von dem übergeordneten Notification Server-Computer aus steuern. Diese globalen Richtlinien können auf jedem untergeordneten Notification Server-Computer in der Hierarchie ausgeführt werden.

Auf dem globalen Notification Server-Computer können Sie globale Berichte erstellen. Damit diese Berichte jedoch die von Ihnen benötigten Daten enthalten, müssen Sie möglicherweise angeben, welche Daten für diese Berichte repliziert werden müssen.

Ein globaler Administrator kann Richtlinien an untergeordnete Notification Server-Computer verteilen, auf denen der lokale Administrator die Richtlinie ändern und anwenden kann. Diese verteilten Richtlinien können als bearbeitbar oder nicht-bearbeitbar festgelegt werden.

Eine nicht-bearbeitbare Richtlinie wird verwendet, um konsistentes Richtlinienverhalten auf allen Notification Server-Computern zu erzwingen. Untergeordnete Administratoren können diese Rechte nur dann überschreiben, wenn Sie die Eigenschaften der Richtlinie angeben, die bearbeitet werden dürfen. Eine bearbeitbare Richtlinie lässt zu, dass untergeordnete Administratoren eine gemeinsame Richtlinie ändern, die für bestimmte Ziele und Zeitpläne gelten soll.

Eine nicht-bearbeitbare Richtlinie kann dupliziert werden. Alle Eigenschaften der duplizierten Richtlinien können dann bearbeitet werden. Ob eine Richtlinie dupliziert werden darf, wird durch rollenbasierte Sicherheitsrechte gesteuert.

Wie Hierarchiereplikation mit Hierarchie funktioniert

Der Zweck der Hierarchie besteht darin, mehrere Notification Server-Computer in einer Symantec Management-Plattform zu kombinieren. Sie ermöglicht es, einige Richtlinien von einer einzelnen Symantec Management Console aus zu verwalten. Allerdings wird durch die Hierarchie nicht die Anzahl der Endgeräte vergrößert, die jeder Notification Server-Computer an sich unterstützen kann.

Beispielsweise können Sie eine Software-Verteilungsrichtlinie replizieren. Durch das Replizieren der Richtlinie werden auch die zugehörigen Daten repliziert. Diese Daten umfassen ein Softwarepaket, damit die Software an die betreffenden Clientcomputer des untergeordneten Notification Server-Computers verteilt werden kann.

In einer Hierarchie können Sie sowohl vom übergeordneten Notification Server-Computer als auch vom untergeordneten Notification Server-Computer aus verwalten. Die vom übergeordneten Server ausgehende Verwaltung betrifft alle untergeordneten Server. Die von einem untergeordneten Server ausgehende betrifft nur die zugehörigen Endgeräte. Diese Funktionalität ermöglicht es, globale und regionale Verwaltungspraktiken auf einer Plattform zu kombinieren. Beispielsweise kann eine globale Richtlinie vom übergeordneten Notification Server-Computer an alle verwalteten Endgeräten verteilt werden. Administratoren des untergeordneten Notification Servers können auch Richtlinien für ihre bestimmte Region erstellen.

Bearbeitbare Eigenschaften der Hierarchie

Bearbeitbare Eigenschaften der Hierarchie ermöglichen dem übergeordneten Administrator, zu steuern, welche Aspekte der replizierten Richtlinien ein untergeordneter Administrator bearbeiten darf. Die Änderungen eines untergeordneten Administrators werden durch nachfolgende Replikationen nicht überschrieben.

Sie können definieren, ob ein Administrator des untergeordneten Notification Servers berechtigt ist, folgende Schritte durchzuführen:

- Aktivieren und Deaktivieren einer globalen Richtlinie.

- Ändern des Zeitplans einer globalen Richtlinie.
- Ändern der Ziele der globalen Richtlinie.

Siehe "Einsatzmöglichkeiten der Hierarchiereplikation" auf Seite 120.

Einsatzmöglichkeiten der Hierarchiereplikation

Hierarchiereplikation liefert begrenzte Möglichkeiten der zentralen Verwaltung. Hierarchiereplikation ist eine Methode, Richtlinien zentral zu verwalten, wenn mehrere Notification Server-Computer erforderlich sind.

Mit Hierarchiereplikation können Sie Folgendes tun:

- Erstellen und verteilen Sie zentrale Richtlinien.
- Replizieren Sie Pakete.
- Leiten Sie Inventar für begrenzte zentrale Berichterstellung weiter.
- Verwalten Sie Sicherheitsrollen zentral.

Siehe "Info zur Hierarchiereplikation" auf Seite 118.

Info zur Hierarchietopologie

Die Hierarchietopologie ist ein Satz von 1:1-Eltern-Kind-Beziehungen zwischen zwei oder mehr Notification Server-Computern. Jeder Notification Server-Computer in der Hierarchie kann mehrere untergeordnete Server haben, aber jeder untergeordnete Server darf nur mit einem einzelnen übergeordneten Server eine Verbindung herstellen. Jeder untergeordnete Notification Server-Computer weiß nur von seinem übergeordneten Computer. Er weiß nicht, dass noch weitere untergeordnete Notification Server vorhanden sind.

Sie können sowohl vom übergeordneten als auch vom untergeordneten Notification Server-Computer aus verwalten. Wenn die Verwaltung von einem übergeordneten Server aus erfolgt, kann sie für alle untergeordneten Server und deren verwaltete Computer gelten. Wenn die Verwaltung von einem untergeordneten Server aus erfolgt, betrifft sie nur die verwalteten Computer des untergeordneten Servers.

Wenn Sie die Beziehungen Ihrer Hierarchietopologie einrichten, müssen Sie immer zwei von ihnen auf einmal hinzufügen: einen über- und einen untergeordneten Computer. Sie müssen für beide Notification Server-Computer über Administratorrechte verfügen. Die Beziehungen können vom untergeordneten oder übergeordneten Server aus aufgebaut werden.

Symantec Management-Plattform verfügt über Sicherheitsberechtigungen zum Bearbeiten der für die Hierarchietopologie relevanten Einstellungen, wie das

Aufbauen von Beziehungen, das Bearbeiten von Zeitplänen und das Konfigurieren von Replikationsregeln. Ihre Administratoren können eine Hierarchie erzwingen, um einzelne Elemente zu replizieren, ohne dass ihnen diese Sicherheitsrolle zugewiesen werden muss.

Siehe "Info zur Hierarchiereplikation" auf Seite 118.

So funktionieren Site Server in einer Hierarchie

Zur Hierarchiereplikation werden Site Services verwendet. Jeder Notification Server-Computer-Standort muss über einen Package Server verfügen, und dieser Server muss Off-Box sein. Sie müssen Package Services angrenzender Notification Server-Computer auf ein verwaltetes Gerät übertragen, das Package Services ausführen kann. Stellen Sie sicher, dass der Site Server, der diese Services ausführt, einem Standort oder Subnetz "zugewiesen" worden ist, zu dem der Notification Server gehört, bevor Sie die Hierarchie einrichten.

Neben dem Site Server muss für jede Site ein Task Server und ein Package Server vorhanden sein. Wenn Sie die Deployment Solution nicht verwenden, dann ist es möglicherweise kosteneffektiv, die Task Services auf dem Notification Server-Computer zu verwenden. Wenn Sie Deployment Solution verwenden, dann müssen Sie einen dedizierten Computer als Host der Task Services und Package Services einsetzen. Dieser Computer wird Startserver im Netzwerk bezeichnet. Jede Site eines Notification Server-Computers muss über einen dedizierten Startserver im Netzwerk verfügen. Wenn Sie einen dedizierten Task Server verwenden, müssen Sie die Standortverwaltung manuell konfigurieren, damit alle Clientcomputer auf die Nutzung des dedizierten Task Servers beschränkt werden.

Siehe "Info zur Hierarchiereplikation" auf Seite 118.

Überlegungen zur Implementierung der Hierarchiereplikation für Software Management Solution

Bevor Sie einen Hierarchiereplikationsplan implementieren, berücksichtigen Sie bestimmte Erwägungen über Software Management Solution.

Im Folgenden werden die Implementierungsaspekte mit Software Management Solution beschrieben:

- Hierarchiereplikation repliziert Richtlinien und Pakete zur Softwarebereitstellung auf untergeordnete Notification Server-Computer zur Verteilung.

- Richtlinien, Filter und Pakete werden automatisch in der Hierarchie nach unten repliziert.
- Software Delivery kann abhängig von der Komplexität der Umgebung 48 Stunden oder mehr dauern.
- Die Replikationsregeln müssen angepasst werden, um die Softwarebestanddetails einzuschließen. Die Details werden für die Berichterstellung benötigt.

Überlegungen zur Implementierung der Hierarchiereplikation für Patch Management Solution

In diesem Abschnitt werden bestimmte Aspekte von Patch Management Solution beschrieben, die bekannt sein sollten, bevor Sie einen globalen Richtlinienverteilungsplan implementieren.

Im Folgenden werden die verschiedenen Implementierungsaspekte mit Patch Management Solution beschrieben:

- Verwenden Sie die Patch-Verwaltung in einer Hierarchie, um Software-Updates in der Hierarchie für die Verteilung nach unten zu replizieren und Berichte über Sicherheitslücken oben in der Hierarchie zu erhalten.
- In einer Hierarchie müssen Patches am übergeordneten Notification Server importiert werden.
- Um Verteilungszeiten herabzusetzen, müssen Replikationszeitpläne die folgende Reihenfolge von Vorgängen berücksichtigen: Patchimportzeitplan; Patchimportreplikationsregel; Site Server-Download; Agent-Update-Intervall.
- Ohne übereinstimmende Zeitpläne dauert die Patchverteilung in der Regel mehr als 48 Stunden.
- Eine Richtlinieneinhaltungübersicht ist alles, was auf dem übergeordneten Notification Server-Computer verfügbar ist. Vollständige Analyseberichte über Sicherheitslücken führen einen Drilldown zu jedem untergeordneten Notification Server durch.

Einschränkungen der Hierarchiereplikation

Hierarchiereplikation in einer Hierarchietopologie ersetzt keine regionalen Verwaltungsnotwendigkeiten. Verstehen Sie einige Einschränkungen und Erwägungen, bevor Sie einen Hierarchiereplikationsplan erstellen.

Eine Hierarchie kann die Verwaltung von mehreren Notification Server-Computern vereinfachen. Jedoch ist durch das Vorliegen mehrerer Notification Server-Computer

nicht notwendigerweise angezeigt, dass Sie eine Hierarchie implementieren sollten. Eine Hierarchie vereinfacht zwar die Verwaltung, erhöht jedoch den Infrastruktur-Overhead der Notification Server-Computer.

Hierarchiereplikation hat die folgenden Einschränkungen:

- Hierarchie bietet keine zentrale Ansicht aller Berichtsdaten in einer Umgebung. In einer Hierarchie müssen Administratoren auf den unter- und übergeordneten Notification Servern verwalten und berichten, um alle Daten anzuzeigen.
- Hierarchie ist kein Ersatz für Organisationsansichten und Gruppen. Hierarchie liefert keine bereichsbasierte Verwaltung in einer Umgebung.
- Hierarchie ist keine Datenreplikationsstrategie für Notification Server-Failover.
- Die Notification Server-Hierarchie unterstützt einen übergeordneten und bis zu sechs untergeordnete Notification Server-Computer. Diese Anzahl hängt von den Hardware-Ausstattung jedes Servers und Ihren IT-Verwaltungsanforderungen ab. Beispielsweise können sich die Häufigkeit und die Menge der Inventardaten, die Sie sammeln, auf die Anzahl der Clients auswirken, die jeder Notification Server-Computer unterstützen kann. In einem sehr komplexen Hierarchienszenario sollten Sie Symantec Consulting Services kontaktieren, um Ihre Anforderungen zu analysieren und die Plattformarchitektur auf Ihre Anforderungen abzustimmen.
- Replikation betrifft die Leistung aller Notification Server-Computer. Diese zusätzliche Last des untergeordneten Notification Server-Computers beeinflusst möglicherweise die maximale Anzahl von Clients, die er unterstützen kann.
- Wenn Replikation mehr als einmal am Tag durchgeführt wird, kann das zusätzlichen Verarbeitungsaufwand für die über- und untergeordneten Notification Server verursachen und ist möglicherweise nicht durchführbar.
- Nicht alle Lösungen in der Symantec Management-Plattform unterstützen die Hierarchiereplikation.
- Auf allen Notification Server-Computern müssen die gleichen Versionen der Symantec Management-Plattform und der Lösungen installiert sein. Um die Version zu ermitteln, können Sie Symantec Installation Manager auf jedem Notification Server-Computer lokal öffnen und die Version verzeichnen.
  Um Symantec Management-Plattform-Updates durchzuführen, muss die Hierarchiereplikation zuerst deaktiviert werden, um Konflikte zwischen verschiedenen Versionen zu vermeiden. Sie können die Hierarchiereplikation auf bestimmten Notification Server-Computern einfach mit einem Schritt aktivieren oder deaktivieren. Zur Durchführung von Lösungsupdates verwenden Sie Symantec Installation Manager lokal auf jedem Notification Server-Computer.
  Weitere Informationen finden Sie in den IT Management Suite-Migrationshandbüchern.

- Die Hierarchiereplikation kann keine Echtzeitdaten liefern. Durch die Übertragung der Daten innerhalb der Hierarchie ergibt sich eine zeitliche Verzögerung. Wenn Sie den Standardzeitplan für die Software-Verteilung verwenden, dann sind für jede Ebene in der Hierarchie bis zu 24 Stunden erforderlich. Sie können die Replikation einzelner Elemente erzwingen, indem Sie jetzt die Option zur sofortigen Replikation verwenden, statt auf die Replikation nach dem Zeitplan zu warten.
- Wenn Clients mit SSL (HTTP oder HTTPS) konfiguriert werden, dann muss der Notification Server-Computer auch entsprechend konfiguriert werden. Umgebungen, in denen sowohl mit als auch ohne SSL gearbeitet wird, sollten nicht unterstützt werden. Wenn ein Notification Server-Computer SSL verwendet, dann müssen alle für SSL konfiguriert werden.
- Asset Management 7.5 und CMDB 7.5 wurden entwickelt, um mit Hierarchie- und eigenständigen Replikationsregeln zu funktionieren. Der Asset Management-/CMDB-Server muss der oberste Server (der übergeordnete) in einer Hierarchie sein. Asset Management/CMDB können sich nicht auf einem untergeordneter Server befinden. Eigenständige Replikationsregeln können Bestand an den Assets Management-/CMDB-Server weiterleiten, aber nicht von diesem Server.

Siehe "Einsatzmöglichkeiten der Hierarchiereplikation" auf Seite 120.

Implementieren der Notification Server-Hierarchie

Damit Sie Konfigurationseinstellungen und Daten mit mehreren Notification Servers gemeinsam nutzen oder anfordern können, müssen Sie den Notification Server-Computer einer Hierarchie hinzufügen und die notwendigen Replikationsregeln konfigurieren.

Tabelle 7-1 Implementieren der Notification Server-Hierarchie

Schritt	Aktion	Beschreibung
Schritt 1	Erstellen Sie die entsprechenden hierarchischen Beziehungen zwischen Notification Servern.	Sie erstellen ein Hierarchie durch Erstellen einer Reihe von Übergeordnet/Untergeordnet- und Untergeordnet/Übergeordnet-Beziehungen, die die Notification Server-Computer in Ihrem System verbinden.

Schritt	Aktion	Beschreibung
Schritt 2	Erstellen und aktivieren Sie die entsprechenden Replikationsregeln zur Angabe der Daten, die durch die Hierarchie repliziert werden sollen.	Die Hierarchiereplikation von Ressourcen und Ereignissen wird mit Hilfe von Replikationsregeln konfiguriert. Diese Regeln definieren die Daten, die auf anderen Notification Servers repliziert werden sollen. Wenn Sie eine benutzerdefinierte Hierarchiereplikation für Konfigurations- und Verwaltungselemente einrichten möchten, nehmen Sie die entsprechenden Einstellungen vor.
Schritt 3	(Optional) Führen Sie die manuellen Replikationsaufgaben aus.	Die in einer Hierarchie enthaltenen Notification Server-Computer werden normalerweise nach dem Replikationszeitplan synchronisiert, der in den Replikationsregeln eingerichtet wurde. Sie können bei Bedarf den Differenzial-Replikationszeitplan für den Notification Server manuell übergehen und die Hierarchiereplikationsregeln sofort auslösen. Sie können auch ausgewählte Daten direkt aus einem Notification Server manuell auf alle ihm untergeordneten Notification Server replizieren, ohne dies in einer Replikationsregel aufzunehmen. Manuelle Replikation ist eine einmalige, sofort stattfindende Replikation. Sie benötigen die Leseberechtigung, damit die Replikation auf über den Kontextmenüeintrag "Jetzt replizieren" durchgeführt werden kann.
Schritt 4	(Optional) Einrichten von Hierarchieautomatisierungsrichtlinien.	Automatisierungsrichtlinien für die Hierarchie senden E-Mail-Benachrichtigungen, wenn bestimmte Ereignisse in der Hierarchie auftreten.
Schritt 5	Ausführen eines Hierarchieberichts.	Sie können einen Bericht auf einem beliebigen Notification Server in der Hierarchie ausführen, um Daten aus dessen CMDB zu extrahieren. Aktualisieren der Zusammenfassungsdaten vor dem Ausführen eines Hierarchieberichts.

Weitere Informationen zum Ausführen der Aufgaben zum Implementieren der Notification Server-Hierarchie finden Sie im Administratorhandbuch zu IT Management Suite.

Info zu Peer-zu-Peer-Replikation und Replikationsregeln

Hinweis: Replikation wird nicht zwischen zwei Notification Server unterstützt, auf denen verschiedene Versionen der IT Management Suite installiert sind. Beispielsweise können Sie Daten von einem 7.0-Server nicht auf einen 7.1-Server replizieren.

Die Peer-zu-Peer-Replikation ist etwas anderes als die Hierarchiereplikation. Die Peer-Replikation definiert den Informationsfluss zwischen zwei Notification Servern. Die Hierarchiereplikation stellt zuverlässige und skalierbare Datensynchronisierung zwischen mehreren Notification Servern zur Verfügung.

Die Replikation kann so konfiguriert werden, dass Daten außerhalb der Hierarchiestruktur repliziert werden. Beispielsweise durch das Senden von Daten zu einem externen Server, der bestimmte Informationen für Berichte sammelt.

Die folgenden Replikationstypen werden unterstützt:

Differenziell	Repliziert Objekte und Daten, die seit der letzten Replikation geändert wurden. Dies ist die empfohlene Methode, weil beim Replizieren von Daten der Verbrauch der Netzwerklast und -bandbreite verringert wird.
Vollständig	Repliziert alle Objekte und Daten. Diese Methode wird häufig für die Hierarchiereplikation verwendet. Eine vollständige Replikation wird im Allgemeinen durch monatliche Durchführung sichergestellt. Die eigenständige Replikation führt im Unterschied zur Hierarchiereplikation keine vollständige Replikation aus. Die eigenständige Replikation ist immer differenzial.

Ein anderer Unterschied zwischen der Hierarchiereplikation und Replikation besteht darin, dass innerhalb einer Hierarchie die replizierten Daten gesichert und (standardmäßig) schreibgeschützt sind. Der Besitz ist zutreffend, so dass untergeordnete Notification Server die Daten, die von den übergeordneten Notification Servern abwärts repliziert wurden, nicht automatisch überschreiben können. Einige Daten enthalten die Einstellungen, wodurch er auf dem Ziel bearbeitet werden kann, und diese können entsprechend konfiguriert werden. Die Replikation hat keinen solchen Besitz, so dass alle replizierten Daten auf den Ziel-Notification Servern bearbeitet werden können.

Um die Replikation zu konfigurieren, müssen Sie auf jedem Notification Server-Computer die entsprechenden Replikationsregeln einrichten. In jeder Regel wird festgelegt, welche Daten von diesem Server (dem Quellserver) auf einen oder mehrere Zielservern repliziert werden und welcher Zeitplan dafür verwendet wird.

Sie können für folgende Elemente eine Replikationsregel erstellen:

Ereignisse	Repliziert Notification Server-Ereignisse.
Elemente	Repliziert Konfigurations- und Verwaltungselemente des Notification Servers, wie Richtlinien, Filter und Berichte.
Ressourcen	Repliziert Notification Server-Ressourcentypen, -Ressourcenziele und spezifische Datenklassen. Wenn Sie Ressourcenziele in eine Ressourcenreplikationsregel einschließen, müssen Sie beachten, dass die Ressourcendefinition sich nur auf den Inhalt (Ressourcen) des replizierten Ziels bezieht. Aus diesem Grund hängen die replizierten Ressourcen vom Eigentümer des Ressourcenziels ab. Der Notification Server-Administrator kann festlegen, dass Ressourcenziele in ihrem aktuellen Status (im Besitz eines anderen Benutzers mit dem entsprechenden Berechtigungsumfang) repliziert werden. Er kann sich auch die Ziele zuweisen, diese mit Administratorumfang speichern (schließt normalerweise mehr Ressourcen ein) und dann in diesem Status replizieren. Alle aktuellen Elemente eines Ressourcenziels werden repliziert. Das eigentliche Ressourcenzielelement wird im Hintergrund als abhängiges Objekt repliziert. Das Ziel, das auf eine eigenständige Regel angewendet wird, wird ebenfalls repliziert, wenn die eigenständige Regel repliziert wird. Wenn die Regel ausgeführt wird, wird das Ziel nicht gesendet.
Sicherheit	Repliziert Notification Server-Sicherheitsrollen und -rechte. Es stehen zwei Arten von Sicherheits-Replikationsregeln zur Verfügung: Recht und Rolle. Die Konfigurationsverfahren für beide sind identisch. Wenn Sie eine Sicherheitsrolle in einer Replikationsregel einschließen, müssen Sie auch eine Replikationsregel konfigurieren, um alle Rechte in der Rolle zu replizieren. Die replizierte Sicherheitsrolle erkennt keine der Privilegien an, die bereits auf dem Notification Server-Zielcomputer bestehen.

Hierarchiereplikationsregeln

Die Hierarchiereplikation beruht auf Replikationsregeln. Diese Regeln definieren die Daten, die auf andere Notification Server-Computer repliziert werden. Viele Elemente werden so konfiguriert, dass sie standardmäßig replizieren werden. Es

gibt jedoch praktische Beschränkungen, insbesondere bezüglich der Anzahl von Elementen, die in der Hierarchie nach oben repliziert werden können. Beispielsweise sind viele Inventardatenklassen standardmäßig nicht in der Lage, in der Hierarchie nach oben zu replizieren. Ohne diese Datenklassen können einige Berichte nicht auf dem übergeordneten Notification Server-Computer ausgeführt werden. Sie sollten sehr sorgfältig auswählen, welche Datenklassen nach oben repliziert werden sollen. Replikationsregeln können jederzeit deaktiviert und später wieder aktiviert werden, sie werden nicht gelöscht.

Ereignisse sind ein anderes Element, dessen Replikation einen übergeordneten Notification Server-Computer überlasten kann. Standardmäßig werden keine Ereignisse für die Replikation aktiviert. Diese sollten nur mit großer Vorsicht und für begrenzte Zeiträume repliziert werden. Beachten Sie, dass die Replikation nicht in Echtzeit erfolgt und die Ereignisdaten daher nicht zur Ausgabe von Alarmen auf dem übergeordneter Notification Server-Computer verwendet werden können.

Informationen zur MultiCMDB-Berichtserstellung mit IT Analytics

IT Analytics schließt eine neue Funktion namens MultiCMDB ein. Mit MultiCMDB können Sie globale IT Analytics-Berichte über mehrere CMDBs hinweg ausführen. Sie brauchen keine großen Datenmengen zu replizieren. Sie können vorhandene Cubes von vielen Notification Server-Computern ausfüllen. Es ist nicht von Bedeutung, ob Notification Server in einer Hierarchie oder eigenständig konfiguriert sind. MultiCMDB unterstützt Verbindungen mit externen 7.0- und 7.5-CMDBs. Sie können die Cubes aktivieren, für die Sie Daten zur Verfügung haben, und andere nicht aktivieren. Mit dieser Funktion können Sie CMDBs mit verschiedenen installierten Lösungen verwenden. Sie müssen nicht konsistent sein.

Sie können derzeit keine Filter (z. B. für Richtlinienziele) aus den ITA-Berichten erstellen. MultiCMDB bietet zwar eine Berichtserstellung, jedoch keine Verwaltung von oben nach unten. Sie sollten auch beachten, dass die MultiCMDB-Funktion keine Berichtserstellung mit den ServiceDesk-Daten unterstützt. Die MultiCMDB-Funktion umfasst nur Daten, die in einer Symantec CMDB vorhanden sind. ServiceDesk verwendet eine separate Datenbank

IT Analytics MultiCMDB kann Folgendes zur Verfügung stellen:

- Eine leistungsfähige, globale ITA-Berichtserstellung über mehrere CMDBs in Umgebungen ohne Hierarchie hinweg.
  MultiCMDB ersetzt keine Hierarchie. Es ermöglicht eine globale IT Analytics-Berichtserstellung, ohne dass große Datenmengen repliziert werden müssen. Eine Hierarchie wird weiterhin für die Verwaltung von Spitzenanwendungsfällen benötigt. Die MultiCMDB-Funktion erkennt die

Hierarchie nicht automatisch. Sie müssen IT Analytics manuell auf alle CMDBs verweisen, für die Sie die ITA-Berichtserstellung ausführen möchten. Dieser Vorgang kann auf der IT Analytics-Konfigurationsseite durchgeführt werden.

- Leistungsstarke, globale ITA-Berichtserstellung über mehrere CMDBs in Umgebungen mit Hierarchie hinweg.
  Sie müssen Ihre Aufmerksamkeit darauf richten, ob Sie den Knoten der obersten Hierarchieebene in die globale Berichtserstellung einschließen möchten. Sie sollten den Knoten der obersten Ebene aus der MultiCMDB ausschließen, wenn der Server der obersten Ebene zum Empfangen von Daten von einer untergeordneten Ebene verwendet wird. Das Ausschließen des obersten Knotens trägt zum Lösen eines Asset-Duplizierungsproblems bei. Derzeit ist diese Funktion keine gute Wahl für die hierarchischen Umgebungen, die die Asset Management Solution verwenden.
- Leistungsfähige, globale ITA-Berichterstellung während der Migration von Version 7.0 auf 7.5 (mindestens ein Server verfügt über Version 7.5 und die übrigen Server über 7.0), mit oder ohne Hierarchie.
  Sie können die Funktion "MultiCMDB" während der Migration der IT Management Suite von Version 7.0 auf 7.5 verwenden. Mit der Funktion "MultiCMDB" können Sie einen Bericht über eine Mischung aus 7.0- und 7.5-Daten erstellen. Diese Berichterstellung kann hilfreich sein, wenn die Umgebung die Hierarchie nutzt, weil die Hierarchie während einer Migration von Version 7.0 auf 7.5 neu erstellt werden muss.
- Multi-CMDB-Cube-Einschluss
  Die Funktion des Cube-Einschlusses ermöglicht es einem Benutzer, auszuwählen, welches CMDBs für jeden Cube verarbeitet werden soll. Durch die Auswahl der CMDB wird das Problem der Datenduplizierung gelöst, da der Benutzer die übergeordnete CMDB effektiv von allen inventarspezifischen Cubes ausschließen und nur die übergeordnete CMDB für die assetspezifischen Cubes verarbeiten kann. Darüber hinaus können die untergeordneten CMDBs konfiguriert werden, um nur im Bereich für die inventarbasierten Cubes (Computer, Patch) zu sein.

Anhang A

Symantec IT Management Suite – Plattformunterstützungsmatrix

Dieser Anhang enthält folgende Themen:

- Einleitung
- Symantec Management-Plattform
- Client Management Suite
- Server Management Suite
- Deployment Solution
- Sprachunterstützung

Einleitung

Die Symantec IT Management Suite Platform Support Matrix (PSM) ist erstellt worden, um aktuelle und zukünftige geplante Plattformstützinformationen zur Verfügung zu stellen. Sie ist so organisiert, dass die Informationen basierend auf den Symantecs IT Management Suite (ITMS)-Komponenten sowie durch ITMS-Version angezeigt werden.

Viele Betriebssystem- und Datenbankplattformen umfassen mehrere Versionen, die auf dem gleichen Plattformkern basieren. Ein Beispiel dafür ist Windows Vista mit Home Basic, Home Premium, Business und Ultimate. QS-Prüfungsressourcen sind begrenzt. Deshalb bieten wir nur eine Plattform im PSM an, wenn diese Plattform tatsächlich getestet worden ist. Dadurch wird nicht unbedingt verhindert,

dass andere Plattformen von Kunden verwendet werden. Diese nicht getesteten Plattformen werden allerdings nicht unterstützt.[1]

Alle künftigen Pläne für Produkte sind noch verfrüht. Alle zukünftigen Freigabetermine sind vorläufig und Änderungen vorbehalten. Jede zukünftige Version des Produkts oder geplante Änderungen zu Produktfunktionen unterliegen fortlaufenden Bewertungen von Symantec und sollten nicht als Grundlage für eine Kaufentscheidung dienen

Sollten Änderungen vorgenommen werden, wird eine aktualisierte Version dieses Dokuments zur Verfügung gestellt.

Hinweis: PSM beinhaltet Unterstützung für die Symantec-Lösungen, die derzeit in Client Management Suite (CMS). Server Management Suite (SMS) oder IT Management Suite (ITMS) enthalten sind. Weitere Supportinformation zu Symantec-Lösungen finden Sie in den Versionshinweisen, die mit jeder Lösung veröffentlicht werden.

---

[1] Anfragen zur Unterstützung von derzeit nicht getesteten Plattformen werden als Verbesserungsvorschlag gesehen. Es wird abgewogen, wie viele Kunden davon profitieren können und ob sich der Aufwand an QS und Entwicklung führ eine derartige Unterstützung lohnt

Symantec Management-Plattform

Der folgende Abschnitt enthält die Microsoft-Plattformunterstützung für Symantec Management-Plattform. Dieser Abschnitt beschreibt, welche Plattformen für die Installation von Symantec Management-Plattform-Komponenten unterstützt werden. Weitere Informationen zu unterstützten Agentplattformen finden Sie in den Abschnitten zu Symantec Client Management Suite und Server Management Suite, die später in diesem Dokument bereitgestellt werden.

Notification Server und Workflow-Server

Tabelle A-1 Notification Server und Workflow-Server

Microsoft Server-Betriebssysteme	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
Windows Server 2003				
Windows Server 2003 SP2 x86	Unterstützt	Unterstützt	Nicht unterstützt	Nicht unterstützt

Microsoft Server-Betriebssysteme	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
Windows Server 2003 R2 x86	Unterstützt	Unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Server 2003 R2 SP2 x86	Nicht unterstützt	Unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Server 2008				
Windows Server 2008 R2[1]	Nicht unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R2 SP1[1]	Nicht unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R2 SP2[1,2]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Server 2012	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

[1] Symantec Management-Plattform 7.1 unterstützt Windows Server 2008 R2 (nur 64-Bit) Enterprise, Standard und Datacenter Edition. Core Edition wird nicht unterstützt.

[2] Da Microsoft noch keinen Veröffentlichungstermin für Windows Server 2008 R2 SP2 angekündigt hat, ist für diese Version noch keine Unterstützung verfügbar.

Hinweis: Workflow Server enthält die Komponenten "Workflow Server" und "Prozessmanager". Der Abschnitt zu Designer und Tools beinhaltet die Unterstützung für Workflow Designer.

Tabelle A-2 Notification Server auf einem virtuellen Host

Version des virtuellen Host	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
VMware ESX 3.5	Unterstützt	Unterstützt	Unterstützt	Unterstützt
VMware ESX 4.0	Unterstützt	Unterstützt	Unterstützt	Unterstützt
VMware ESX 5.0	Nicht unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
VMware ESX 5.1	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt
Windows Hyper-V Server 2008 R2[1]	Nicht unterstützt	Nicht unterstützt	Unterstützt	Unterstützt

Version des virtuellen Host	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
Windows Hyper-V Server 2012	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt

[1] Beachten Sie, dass für Core-Hyper-V-Server 2008 die Benutzerzugriffssteuerung (UAC) auf eine niedrigere Stufe (1 Stufe unter der maximalen Sicherheitsstufe) eingestellt werden muss, damit Symantec Management Agent funktionieren kann.

Hinweis: Weitere Informationen zum Einrichten von Notification Server auf einem virtueller Host finden Sie im in der Supportdatenbank unter "Installieren der Symantec Management Platform unter VMware":

http://www.symantec.com/docs/HOWTO9692

Microsoft SQL Server

Tabelle A-3 Microsoft SQL Server

Microsoft SQL Server-Version	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
Microsoft SQL Server 2005				
Microsoft SQL Server 2005 SP2	R5	Unterstützt	Unterstützt	Produkteinstellung
Microsoft SQL Server 2005 SP3	R10	Unterstützt	Unterstützt	Produkteinstellung
Microsoft SQL Server 2005 SP4	R13	Nicht unterstützt	Unterstützt	Unterstützt
Microsoft SQL Server 2008				
Microsoft SQL Server 2008	R13	Unterstützt	Unterstützt	Produkteinstellung
Microsoft SQL Server 2008 SP1	Nicht unterstützt	Unterstützt	Unterstützt	Produkteinstellung
Microsoft SQL Server 2008 SP2	Nicht unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Microsoft SQL Server 2008 SP3	Nicht unterstützt	Nicht unterstützt	Unterstützt	Unterstützt

Microsoft SQL Server-Version	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
Microsoft SQL Server 2008 R2*	Nicht unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Microsoft SQL Server 2008 R2 SP1	Nicht unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Microsoft SQL Server 2008 R2 SP2	Nicht unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Microsoft SQL Server 2012				
Microsoft SQL Server 2012	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt
Microsoft SQL Server 2012 SP1	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt

* Wenn R2 SQL 2008 unterstützt wird, wird auch das kumulative Rollup 4 unterstützt.

Hinweis: Die Installation des Notification Server-Computers wird mit den Versionen Microsoft SQL Express, -Standard und -Enterprise x86 und 64-Bit getestet. Bei Verwendung eines 64-Bit-Betriebssystems mit einer x64-Version von SQL Server wird für zugehörige SQL-Server mit mehr als 4 GB physischen Arbeitsspeicher empfohlen, die Speicherfunktionen der 64-Bit-Hardware zu nutzen. Zusätzliche Information finden Sie in folgendem Artikel:

http://www.symantec.com/docs/HOWTO10723

Microsoft SQL Server Collations

Tabelle A-4 Microsoft SQL Server Collations

Microsoft SQL Server Collations	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
Latin1_General_BIN	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Latin1_General_BIN2	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Latin1_General_CI_AI	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Latin1_General_CI_AS	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Latin1_General_CS_AI	Unterstützt	Unterstützt	Unterstützt	Unterstützt

Microsoft SQL Server Collations	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
Latin1_General_CS_AS	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Latin1_General_CP1_CI_AS	Unterstützt	Unterstützt	Unterstützt	Unterstützt

Microsoft IIS

Tabelle A-5 Microsoft IIS

IIS-Version	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
Microsoft IIS 6	Unterstützt	Unterstützt	Nicht unterstützt	Nicht unterstützt
Microsoft IIS 7.5 (IISs 6-Kompatibilität)	Nicht unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Microsoft IIS 7.5 Native	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Microsoft IIS 8 Native[1]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

[1]Zur Zeit der Veröffentlichung dieses Dokuments war IIS 8 noch nicht veröffentlicht.

Microsoft .NET

Tabelle A-6 Microsoft .NET

.NET-Version	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
Microsoft .NET Framework 1.1	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Microsoft .NET Framework 3.5	Nicht unterstützt	Unterstützt	Nicht unterstützt	Nicht unterstützt
Microsoft .NET Framework 3.5 SP1	Nicht unterstützt	Unterstützt	Unterstützt	Unterstützt
Microsoft .NET Framework 4.0	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

Konsole/Browser

Tabelle A-7 Konsole/Browser

Browser-Version	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
Microsoft Internet Explorer 6 SP1	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Microsoft Internet Explorer 7	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Microsoft Internet Explorer 8 (nur Kompatibilitätsmodus)[3]	Nicht unterstützt	Unterstützt	Unterstützt	Unterstützt
Microsoft Internet Explorer 8	Nicht unterstützt	Unterstützt	Unterstützt	Unterstützt
Microsoft Internet Explorer 9 (nur Kompatibilitätsmodus)[3]	Nicht unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Microsoft Internet Explorer 9[1]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Microsoft Internet Explorer 10 (nur Kompatibilitätsmodus)[3]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Eingeschränkte Unterstützung [2]
Microsoft Internet Explorer 10	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Microsoft Internet Explorer 11[4]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

Hinweis: Aktuell referenzierte Browserunterstützung ist für die 32-Bit-Version von Internet Explorer verfügbar.

[1] Wegen der Version von Internet Explorer 10, wird die Unterstützung für den systemeigen Internet Explorer 9 nicht hinzugefügt. Benutzer können Internet Explorer 9 im Kompatibilitätsmodus verwenden.

[2] Es wird nur das Softwareportal "Self-Service" unterstützt. Benutzer ihre Browser nicht in den Kompatibilitätsmodus wechseln, weil Internet Explorer automatisch in den Kompatibilitätsmodus wechselt, wenn das Portal gestartet wird.

[3] Sobald ein Browser vollständig unterstützt wird, wird er im Kompatibilitätsmodus nicht mehr unterstützt. An diesem Punkt wird der Kompatibilitätsmodus in einem Browser nicht mehr unterstützt.

[4]Zur Zeit der Veröffentlichung dieses Dokuments war Internet Explorer 11 noch nicht veröffentlicht.

Workflow Designer

Workflow-Designer und Workflow Tools sind die Client-Tools für Design-, Veröffentlichungs- und Debug-Prozesse. Die folgende Matrix definiert die Microsoft-Plattformen, auf denen Workflow Designer und Workflow Tools unterstützt sind.

Tabelle A-8 Designer und Tools

Betriebssysteme von Microsoft Windows	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
Windows XP				
Windows XP SP2 x86/x64	Unterstützt	Unterstützt	Unterstützt	Produkteinstellung
Windows XP SP3 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Vista				
Windows Vista x86/x64	Unterstützt	Unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Vista SP1 x86/x64	Unterstützt	Unterstützt	Unterstützt	Produkteinstellung
Windows Vista SP2 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows 7				
Windows 7 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows 7 SP1 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows 7 SP2 x86/x64 [1]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Server 2003				
Windows Server 2003 R2 x86/x64	Unterstützt	Unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Server 2003 R2 SP2 x86/x64	Nicht unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008				
Windows Server SP2 2008 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt

Betriebssysteme von Microsoft Windows	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
Windows Server 2008 R1 SP2	Nicht unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R2 SP2[1]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

[1] Microsoft hat noch keinen Veröffentlichungstermin für Windows 7 SP2 oder Windows Server 2008 R2 SP2 angekündigt. Aus diesem Grund wurde für diese Versionen keine Unterstützung hinzugefügt.

Site Server

Server, auf denen entweder Package Service oder Task Service installiert ist, werden "Site Server" genannt. In der folgenden Site Server-Unterstützungstabelle ist von der vollständigen Unterstützung von Package Service und Task Service auf der jeweiligen Plattform auszugehen, falls nicht anders angegeben. Diese Dienste können auch unter beliebigen unterstützten Notification Server-Betriebssystemen ausgeführt werden.

Tabelle A-9 Site Server-Betriebssystemunterstützung

Site Server-Betriebssysteme	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
Windows 2000				
Windows Server 2000 SP4	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows 2000 Professional SP4	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows XP				
Windows XP SP2 x86/x64[1]	Unterstützt	Unterstützt	Unterstützt	Ende des Lebenszyklus
Windows XP SP3 x86/x64[1]	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Vista				
Windows Vista x86/x64[1]1	Nicht unterstützt	Nur Package Server	Nicht unterstützt	Nicht unterstützt
Windows Vista SP1 x86/x64[1]	Nicht unterstützt	Nur Package Server	Nur Package Server	Ende des Lebenszyklus

Site Server-Betriebssysteme	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
Windows Vista SP2 x86/x64[1]	R13	Unterstützt	Unterstützt	Unterstützt
Windows 7				
Windows 7 x86/x64[1]	R13	Unterstützt	Unterstützt	Unterstützt
Windows 7 SP1 x86/x64 [1]	R13	Nicht unterstützt	Unterstützt	Unterstützt
Windows 7 SP2 x86/x64 [1]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows 8				
Windows 8	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Server 2003				
Windows Server 2003 SP2 x86	R5	Unterstützt	Unterstützt	Unterstützt
Windows Server 2003 SP2 x64[1]	R9	Unterstützt	Unterstützt	Unterstützt
Windows Server 2003 R2 x86/x64[1]	Unterstützt	Unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Server 2003 R2 SP2 x86/x64[1]	Nicht unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008				
Windows Server 2008 x86/x64[1]	R8	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 SP2 x86/x64[1]	R13	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R2	R13	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R2 Core	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Server 2008 R1 SP2	R13	Nicht unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R2 SP2[3]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Server 2012				

Site Server-Betriebssysteme	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
Windows Server 2012	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Red Hat Enterprise Linux 4				
Red Hat Enterprise Linux 4 WS x86/x64	Nur Package Server[2]	Nicht unterstützt	Nur Package Server[2]	Ende des Lebenszyklus
Red Hat Enterprise Linux 4 ES x86/x64	Nur Package Server[2]	Nicht unterstützt	Nur Package Server[2]	Ende des Lebenszyklus
Red Hat Enterprise Linux 4 AS x86/x64	Nur Package Server[2]	Nicht unterstützt	Nur Package Server[2]	Ende des Lebenszyklus
Red Hat Enterprise Linux 5				
Red Hat Enterprise Linux 5.1 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Nur Package Server	Nur Package Server
Red Hat Enterprise Linux 5.2 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Nur Package Server	Nur Package Server
Red Hat Enterprise Linux 5.3 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Nur Package Server	Nur Package Server
Red Hat Enterprise Linux 5.4 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Nur Package Server	Nur Package Server
Red Hat Enterprise Linux 5.5 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Nur Package Server	Nur Package Server
Red Hat Enterprise Linux 5.6 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Nur Package Server	Nur Package Server
Red Hat Enterprise Linux 5.7 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nur Package Server
Red Hat Enterprise Linux 5.8 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nur Package Server
Red Hat Enterprise Linux 6				
Red Hat Enterprise Linux 6.0 x86/x64	Nicht unterstützt	Nicht unterstützt	Unterstützt	Nur Package Server
Red Hat Enterprise Linux Server 6.0 x86/x64	Nicht unterstützt	Nicht unterstützt	Unterstützt	Nur Package Server

Site Server-Betriebssysteme	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
Red Hat Enterprise Linux 6.1 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Unterstützt	Nur Package Server
Red Hat Enterprise Linux 6.2 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nur Package Server
Red Hat Enterprise Linux 6.3 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt
Novell SUSE Enterprise Server				
Novell SUSE Linux Enterprise Server 9 x86/x64	Nur Package Server	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Novell SUSE Linux Enterprise Server 10 x86/x64	Nur Package Server	Nicht unterstützt	Nur Package Server	Nur Package Server
Novell SUSE Linux Enterprise Server 11 x86/x64	Nicht unterstützt	Nicht unterstützt	Nur Package Server	Nur Package Server
Novell SUSE Linux Enterprise Server 11 SP1 x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nur Package Server
Novell SUSE Linux Enterprise Server 11 SP2 x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nur Package Server
Sun Solaris				
Sun Solaris 7 SPARC	Nur Package Server	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Sun Solaris 8 SPARC	Nur Package Server	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Sun Solaris 9 SPARC	Nur Package Server	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Sun Solaris 10 x86/x64/Sparc	Nur Package Server	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
IBM AIX				
IBM AIX 4.3	Nur Package Server	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
IBM AIX 5.1 PPC	Nur Package Server	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
IBM AIX 5.2 PPC	Nur Package Server	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
IBM AIX 5.3 PPC	Nur Package Server	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Hewlett-Packard HP-UX				

Site Server-Betriebssysteme	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
Hewlett-Packard HP-UX 11 PA-RISC/IA-64	Nur Package Server	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Hewlett-Packard HP-UX 11i PA-RISC/IA-64	Nur Package Server	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

[1] Beachten Sie, dass die 6.x-Core-Agents, die auf x64-Plattformen ausgeführt werden, derzeit nur auf WOW64 (32-Bit-Emulationsmodus) unterstützt werden. Dadurch kann der Core-Agent nur die Dateien und Registrierungseinträge in der 32-Bit-Umgebung erkennen. Beginnend mit Notification Server 7.1, fügt Symantec Management Agent nativen 64-Bit-Support hinzu.

[2] Der Package Service unterstützt Red Hat Enterprise Linux 4 WS x86/x64 und Novell SUSE Linux Enterprise Desktop Version 10 und 11, wenn Apache Web Server installiert ist. Apache Web Server ist nicht standardmäßig unter diesen Betriebssystemen installiert.

[3] Da Microsoft noch keinen Veröffentlichungstermin für Windows Server 2008 R2 SP2 angekündigt hat, ist für diese Version noch keine Unterstützung verfügbar.

Cloud-fähige Verwaltung (bisher IBCM)

Cloud-fähige Verwaltung (CEM, Cloud Enabled Management) ist eine neue Funktion, die in zukünftigen Releases verfügbar sein wird. Dadurch wird die Verwaltung von Clientcomputern über das Internet mithilfe eines Software-Gateways in der DMZ unterstützt. Der folgende Abschnitt enthält Informationen zur Betriebssystemunterstützung für den Gateway-Server. CEM-Client unterstützt die folgenden Windows Desktop-Betriebssysteme

Tabelle A-10 Internet-Gateway

Microsoft Server-Betriebssysteme	SMP 6.x	SMP 7.0 SP5	SMP 7.1 SP2 MP1.1	SMP 7.5
Windows Server 2008 R1 SP2 x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt
Windows Server 2008 R2 SP1 x64 [1]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Server 2012	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

[1] Microsoft hat noch kein Veröffentlichungsdatum für Windows Server 2008 R2 SP2 angegeben, sodass noch keine Unterstützung für diese Version verfügbar ist.

Hinweis: Internet-Gateway erfordert .NET 3.5 SP1 sowie 64-Bit-Betriebssystem-Plattform.

Client Management Suite

Der folgende Abschnitt enthält die unterstützten Betriebssysteme für die Lösungen der Client Management Suite (CMS). Falls nicht anders angegeben, unterstützt die Suite folgende Lösungen:

- Deployment Solution[6]
- Inventory für Netzwerkgeräte
- Network Discovery
- Out of Band Management
- Patch Management Solution,
- pcAnywhere Solution
- Real-Time System Manager
- Software Management Solution

Client-Betriebssystemunterstützung

Tabelle A-11 Client-Betriebssystemunterstützung

Agent auf Client-Betriebssystemen	6.x	7.0 SP5	7.1 SP2 MP1.1	7.5
Windows 2000				
Windows 2000 Professional SP4	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows XP				
Windows XP Professional SP2 x86	Unterstützt	Unterstützt	Unterstützt	Ende des Lebenszyklus
Windows XP Professional SP2 x64	R9	Unterstützt	Unterstützt	Ende des Lebenszyklus

Agent auf Client-Betriebssystemen	6.x	7.0 SP5	7.1 SP2 MP1.1	7.5
Windows XP Professional SP3 x86	R8	Unterstützt	Unterstützt	Unterstützt
Windows XP Tablet PC Edition 2005	R8	Begrenzte Unterstützung [2]	Begrenzte Unterstützung [2]	Begrenzte Unterstützung [2]
Windows XP Embedded				
Windows XP Embedded SP3	Nicht unterstützt	Begrenzte Unterstützung [2]	Begrenzte Unterstützung [2]	Begrenzte Unterstützung [2]
Windows Embedded Standard	Nicht unterstützt	Begrenzte Unterstützung [2]	Begrenzte Unterstützung [2]	Begrenzte Unterstützung [2]
Windows Embedded Point of Service 1.0	Nicht unterstützt	Begrenzte Unterstützung [2]	Begrenzte Unterstützung [2]	Ende des Lebenszyklus
Windows Embedded Point of Service 1.1 SP3	Nicht unterstützt	Begrenzte Unterstützung [2]	Begrenzte Unterstützung [2]	Begrenzte Unterstützung [2]
Windows Embedded POSReady 2009	Nicht unterstützt	Begrenzte Unterstützung [2]	Begrenzte Unterstützung [2]	Begrenzte Unterstützung [2]
Windows Vista				
Windows Vista x86/x64[1]	Unterstützt	Unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Vista SP1 x86/x64[1]	R8	Unterstützt	Unterstützt	Ende des Lebenszyklus
Windows Vista SP2 x86/x64[1]	R10	Unterstützt	Unterstützt	Unterstützt
Windows 7				
Windows 7 x86/x64[1]	R13	Unterstützt	Unterstützt	Unterstützt
Windows 7 x86/x64 SP1 x86/x64	R13	Nicht unterstützt	Unterstützt	Unterstützt
Windows 7 x86/x64 SP2 x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows 7 XP Mode	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung	Begrenzte Unterstützung
Windows 7 Embedded				

Agent auf Client-Betriebssystemen	6.x	7.0 SP5	7.1 SP2 MP1.1	7.5
Windows 7 Embedded Standard x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt [2]
Windows 7 Embedded Standard x86/x64 SP1	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt [2]
Windows 7 Embedded POSReady 7	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt [2]
Windows 8				
Windows 8	Nicht unterstützt	Nicht unterstützt	Unterstützt [12]	Unterstützt
Windows 8.1 [13]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Red Hat Enterprise Linux 3				
Red Hat Enterprise Linux 3 WS x86/x64	Begrenzte Unterstützung [4]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Red Hat Enterprise Linux 4				
Red Hat Enterprise Linux 4 WS x86/x64	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]	Ende des Lebenszyklus
Red Hat Enterprise Linux 5				
Red Hat Enterprise Linux 5 x86/x64	Nicht unterstützt	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]
Red Hat Enterprise Linux 5.1 x86/x64	Nicht unterstützt	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]
Red Hat Enterprise Linux 5.2 x86/x64	Nicht unterstützt	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]
Red Hat Enterprise Linux 5.3 x86/x64	Nicht unterstützt	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]
Red Hat Enterprise Linux 5.4 x86/x64	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]
Red Hat Enterprise Linux 5.5 x86/x64	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]
Red Hat Enterprise Linux 5.6 x86/x64	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]

Agent auf Client-Betriebssystemen	6.x	7.0 SP5	7.1 SP2 MP1.1	7.5
Red Hat Enterprise Linux 5.7 x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [4]
Red Hat Enterprise Linux 5.8 x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [4]
Red Hat Enterprise Linux 5.9 x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [4, 15]
Red Hat Enterprise Linux 6				
Red Hat Enterprise Linux 6.0 x86/x64	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]
Red Hat Enterprise Linux 6.1 x86/x64	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]
Red Hat Enterprise Linux 6.2 x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [4]
Red Hat Enterprise Linux 6.3 x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [4]
Red Hat Enterprise Linux 6.4 x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [4, 15]
Novell SUSE Linux Enterprise Desktop				
Novell SUSE Linux Enterprise Desktop 10 x86/x64	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]
Novell SUSE Linux Enterprise Desktop 11 x86/x64	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]
Novell SUSE Linux Enterprise Desktop 11 SP1 x86/x64	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]
Novell SUSE Linux Enterprise Desktop 11 SP2 x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [4]
Apple Mac OS X				
Apple Mac OS X (10.2) PPC	Begrenzte Unterstützung [5]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Apple Mac OS X (10.3) PPC	Begrenzte Unterstützung [5]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

Agent auf Client-Betriebssystemen	6.x	7.0 SP5	7.1 SP2 MP1.1	7.5
Apple Mac OS X (10.4) Universal	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]	Ende des Lebenszyklus
Apple Mac OS X (10.5) Universal	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]	Ende des Lebenszyklus
Apple Mac OS X (10.6)	Begrenzte Unterstützung [8]	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]
Apple Mac OS X (10.7)	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [5, 7]	Begrenzte Unterstützung [5]
Mac OS X (10.8)[9]	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [5, 11]	Begrenzte Unterstützung [5, 11]
Mac OS X (10.9)[14]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

[1] Beachten Sie, dass die 6.x-Core-Agents, die auf Windows-x64-Plattformen ausgeführt werden, derzeit nur unter WOW64 (32-Bit-Emulationsmodus unterstützt werden. Dadurch kann der Core-Agent nur die Dateien und Registrierungseinträge in der 32-Bit-Umgebung erkennen. Beginnend mit Notification Server 7.1, fügt Symantec Management Agent nativen 64-Bit-Support hinzu.

[2] Windows Embedded-Funktionen eingeschränkt.

Infos zu Windows 7 Embedded (CMS 7.1 oder höher) finden Sie im folgenden Artikel:

http://www.symantec.com/docs/TECH190554

Infos zu Windows XP Embedded (CMS 7.0 oder höher) finden Sie im folgenden Artikel:

http://www.symantec.com/docs/HOWTO10921

[3] Microsoft hat die Unterstützung für Windows 2000 am 13. Juli 2010 beendet, folglich wurde die Unterstützung für Windows 2000-Agents in der Version 7.0 SP5 entfernt. Grundlegende Agent-Funktionen mit einem 7.0 SP4-Agent in einer 7.0-Umgebung stellt eingeschränkte Funktionen beim Aktualisieren der Agent-Computer zur Verfügung.

[4] Der Linux-Agent unterstützt PC Transplant, Application Management, Software Virtualization Client, WiseScript, Softwareportal und Application Metering nicht.

[5] Der MacOS-Agent unterstützt PC Transplant, Application Management, Software Virtualization Client, WiseScript und Application Metering nicht.

[6] Weitere Unterstützungsinformationen für Deployment 6.9 finden Sie in folgendem Artikel:

http://www.symantec.com/docs/DOC2079

[7] In 7.1 SP1 ist MacOS X 10.7 nur über ein spezielles Point Fix verfügbar (am 19. September 2011 veröffentlicht). Weitere Infos finden Sie im folgenden Artikel:

http://www.symantec.com/docs/HOWTO58968

[8] Unter NS 6.x, ist die Unterstützung von MacOS X 10.6 auf Symantec Management Agent und Grundinventar begrenzt. Keine der Lösungen unterstützt diese Version. Die Unterstützung von Grundinventar und Symantec Management Agent ist über ein spezielles Point Fix verfügbar. Weitere Infos finden Sie im folgenden Artikel:

http://www.symantec.com/docs/HOWTO21457

[9] Apple nennt sein Betriebssystem nicht mehr "MacOS X", sondern nur noch "OS X".

[10] Version 7.5 unterstützt Software-Erkennungsregeln für OS X.

[11] pcAnywhere Solution wird derzeit nicht unterstützt.

[12] Für die Unterstützung von Microsoft Windows 8 gelten die bekannten Einschränkungen in diesem Artikel:

http://www.symantec.com/docs/DOC6193

[13] Zum Zeitpunkt der Veröffentlichung dieser Version dieses Dokuments war Windows 8.1 noch nicht verfügbar.

[14] Zum Zeitpunkt der Veröffentlichung dieser Version dieses Dokuments war OS X 10.9 (Mavericks) noch nicht verfügbar. Die Veröffentlichung ist für Herbst 2013 geplant.

Server Management Suite

Der folgende Abschnitt enthält die unterstützten Betriebssysteme für die Lösungen der Server Management Suite (SMS). Falls nicht anders angegeben, unterstützt die Suite folgende Lösungen: Deployment Solution[10], Inventory für Netzwerkgeräte, Inventory Solution, Network Discovery, Out of Band Management, Patch Management Solution, Real-Time System Manager, Software Management Solution und Monitor Solution für Server.

Server-Betriebssystemunterstützung

Tabelle A-12 Server-Betriebssystemunterstützung

Agent auf Server-Betriebssystemen	6.x	7.0 SP5	7.1 SP2 MP1.1	7.5
Windows Server 2000				
Windows Server 2000 SP4	Unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Server 2003				
Windows Server 2003 SP2 x86	R5	Unterstützt	Unterstützt	Unterstützt
Windows Server 2003 SP2 x64[1]	R9	Unterstützt	Unterstützt	Unterstützt
Windows Server 2003 R2 x86/x64[1]	Unterstützt	Unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Server 2003 R2 SP2 x86/x64[1]	Nicht unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Small Business Server (SBS) 2003 R2 x86/x64[1]	Nicht unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Windows Server 2008				
Windows Server 2008 x86/x64[1]	R8	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 SP2 x86/x64[1]	R13	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 Core x86/x64[1]	R13	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R2	R13	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R2 Core[3]	R13	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R1 SP2	R13	Nicht unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R2 SP2	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

Agent auf Server-Betriebssystemen	6.x	7.0 SP5	7.1 SP2 MP1.1	7.5
Windows Server 2012	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt
Windows Hyper-V Server 2008	Nicht unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Windows Small Business Server (SBS) 2008	Nicht unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Apple Mac OS X Server				
Apple Mac OS X Server (10.2) PPC	Begrenzte Unterstützung [4]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Apple Mac OS X Server (10.3) PPC	Begrenzte Unterstützung [4]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Apple Mac OS X Server (10.4) Universal	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]	Ende des Lebenszyklus
Apple Mac OS X Server (10.5) Universal	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]	Ende des Lebenszyklus
Apple Mac OS X Server (10.6)	Begrenzte Unterstützung [12]	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4]
Apple Mac OS X Server (10.7)	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [11]	Begrenzte Unterstützung [4]
Apple OS X Server (10.8)[15]	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [4]	Begrenzte Unterstützung [4,14]
Apple OS X Server (10,9)[16]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Red Hat Enterprise Linux 3				
Red Hat Enterprise Linux 3 ES x86/x64	Begrenzte Unterstützung [5]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Red Hat Enterprise Linux 3 AS x86/x64	Begrenzte Unterstützung [5]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Red Hat Enterprise Linux 4				
Red Hat Enterprise Linux 4 ES x86/x64	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]	Ende des Lebenszyklus

Agent auf Server-Betriebssystemen	6.x	7.0 SP5	7.1 SP2 MP1.1	7.5
Red Hat Enterprise Linux 4 AS x86/x64	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]	Ende des Lebenszyklus
Red Hat Enterprise Linux 5				
Red Hat Enterprise Linux 5 Server x86/x64	Nicht unterstützt	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]
Red Hat Enterprise Linux 5.1 Server x86/x64	Nicht unterstützt	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]
Red Hat Enterprise Linux 5.2 Server x86/x64	Nicht unterstützt	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]
Red Hat Enterprise Linux 5.3 Server x86/x64	Nicht unterstützt	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]
Red Hat Enterprise Linux 5.4 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]
Red Hat Enterprise Linux 5.5 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]
Red Hat Enterprise Linux 5.6 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]
Red Hat Enterprise Linux 5.7 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [5]
Red Hat Enterprise Linux 5.8 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [5]
Red Hat Enterprise Linux 5.9 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [5, 17]
Red Hat Enterprise Linux 6				
Red Hat Enterprise Linux 6 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]
Red Hat Enterprise Linux 6.1 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]
Red Hat Enterprise Linux 6.2 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [5]

Agent auf Server-Betriebssystemen	6.x	7.0 SP5	7.1 SP2 MP1.1	7.5
Red Hat Enterprise Linux 6.3 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [5]
Red Hat Enterprise Linux 6.4 Server x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [5, 17]
Novell SUSE Linux Enterprise Server				
Novell SUSE Linux Enterprise Server 8 x86	Begrenzte Unterstützung [5]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Novell SUSE Linux Enterprise Server 9 x86/x64	Begrenzte Unterstützung [5]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Novell SUSE Linux Enterprise Server 10 x86/x64	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]
Novell SUSE Linux Enterprise Server 11 x86/x64	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]
Novell SUSE Linux Enterprise Server 11 SP2 x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [5]
Novell SUSE Linux Enterprise Server 12 x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
VMware vSphere/ESX/ESXi				
VMware ESX/ESXi 3.0.1	Begrenzte Unterstützung [6]	Begrenzte Unterstützung [6]	Nicht unterstützt	Nicht unterstützt
VMware ESX/ESXi 3.0.2	Begrenzte Unterstützung [6]	Begrenzte Unterstützung [6]	Nicht unterstützt	Nicht unterstützt
VMware ESX/ESXi 3.0.3	Begrenzte Unterstützung [6]	Begrenzte Unterstützung [6]	Nicht unterstützt	Nicht unterstützt
VMware ESX/ESXi 3.5	Begrenzte Unterstützung [6]	Begrenzte Unterstützung [6]	Begrenzte Unterstützung [6]	Begrenzte Unterstützung [6]
VMware-vSphere/ESX/ESXi 4.0 (agentenlos)	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [8]	Begrenzte Unterstützung [8]
VMware-vSphere/ESX/ESXi 4.1 (ohne Agent)	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [8]	Begrenzte Unterstützung [8]

Agent auf Server-Betriebssystemen	6.x	7.0 SP5	7.1 SP2 MP1.1	7.5
VMware-vSphere/ESX/ESXi 5.0 (agentenlos)	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [8]	Begrenzte Unterstützung [8]
VMware-vSphere/ESX/ESXi 5.1 (ohne Agent)	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [8]	Begrenzte Unterstützung [8]
Sun Solaris				
Sun Solaris 7 SPARC	Begrenzte Unterstützung [7]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Sun Solaris 8 SPARC	Begrenzte Unterstützung [7]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Sun Solaris 9 SPARC	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]
Sun Solaris 10 x86/x64	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]
Sun Solaris 10 SPARC	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]
Sun Solaris 11 x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Sun Solaris 11 SPARC	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Sun Solaris Zones	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [7,13]	Begrenzte Unterstützung [7]
Hewlett-Packard HP-UX				
Hewlett-Packard HP-UX 11.11 (11i) PA-RISC[9]	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]
Hewlett-Packard HP-UX 11.23 (11i v2) PA-RISC/IA-64[9]	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]
Hewlett-Packard HP-UX 11.31 (11i v3) PA-RISC/IA-64[9]	Nicht unterstützt	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]
Hewlett-Packard HP-UX 11.xx (11i v4) PA-RISC[9]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
IBM AIX				

Agent auf Server-Betriebssystemen	6.x	7.0 SP5	7.1 SP2 MP1.1	7.5
IBM AIX 4.3.3	Begrenzte Unterstützung [7]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
IBM AIX 5.1 PPC	Begrenzte Unterstützung [7]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
IBM AIX 5.2 PPC	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]	Ende des Lebenszyklus
IBM AIX 5.3 PPC	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]	Ende des Lebenszyklus
IBM AIX 6.1 PPC	Nicht unterstützt	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]	Begrenzte Unterstützung [7]
IBM AIX 7.1 Standard	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [7]
IBM LPAR-s	Nicht unterstützt	Nicht unterstützt	Begrenzte Unterstützung [7,13]	Begrenzte Unterstützung [7]

[1] Beachten Sie, dass die 6.x-Core-Agents, die auf x64-Plattformen ausgeführt werden, derzeit nur auf WOW64 (32-Bit-Emulationsmodus) unterstützt werden. Dadurch kann der Core-Agent nur die Dateien und Registrierungseinträge in der 32-Bit-Umgebung erkennen. Beginnend mit Notification Server 7.1, fügt Symantec Management Agent nativen 64-Bit-Support hinzu.

[2] Microsoft hat die Unterstützung für Windows 2000 am 13. Juli 2010 beendet, folglich wurde die Unterstützung für Windows 2000-Agents in der Version 7.0 SP5 entfernt. Grundlegende Agent-Funktionen mit einem 7.0 SP4-Agent in einer 7.0-Umgebung stellt eingeschränkte Funktionen beim Aktualisieren der Agent-Computer zur Verfügung.

[3] "Monitor Pack for Servers" unterstützt nur die Überwachung von Windows Server 2008 R2 Core Edition-Server ohne Agent.

[4] Der Mac OS X-Agent unterstützt PC Transplant, Monitor Solution, Application Management, Software Virtualization Client, WiseScript und Application Metering nicht.

[5] Der Linux-Agent unterstützt PC Transplant, Application Management, Software Virtualization Client, WiseScript, Softwareportal und Application Metering nicht.

[6] VMware ESX und ESXi 3.x unterstützt nur Inventory für Netzwerkgeräte, Inventory Solution, Network Discovery auf Hardwareebene und Monitor Solution.

[7] Der UNIX-Agent unterstützt PC Transplant, Application Management, Software Virtualization Client, WiseScript, Softwareportal, Application Metering und Patch Management nicht.

[8] VMware ESX und ESXi 4 unterstützen nur Inventory for Network Devices und Network Discovery. Beginnend mit Symantec Management-Plattform 7.1, werden ESX- und ESXi-4.x Server als agentenlos verwaltet.

[9] IA-64-Unterstützung auf NS 6.x wird bereitgestellt, indem PA-RISC-Binärdateien unter der HP-UX Aries-Übersetzungsengine ausgeführt werden, die als Core-Komponente von HP-UX bereitgestellt wird. IA-64-Unterstützung mit der Version 7.x wird nativ bereitgestellt.

[10] Weitere Informationen zu Deployment 6.9 finden Sie in folgendem Artikel:

http://www.symantec.com/docs/DOC2079

[11] In 7.1 SP1 ist Mac OS X 10.7 nur über eine spezielle Punktfehlerbehebung verfügbar, die am 19. September 2011 veröffentlicht wurde. Weitere Information finden Sie in folgendem Artikel: http://www.symantec.com/docs/HOWTO58968

[12] Unter NS 6.x, ist die Unterstützung von MacOS X 10.6 auf Altiris Agent und Grundinventar begrenzt. Keine der Lösungen unterstützt diese Version. Die Unterstützung von Grundinventar und Altiris Agent ist über ein spezielles Point Fix verfügbar. Weitere Infos finden Sie im folgenden Artikel:

http://www.symantec.com/docs/HOWTO21457

[13] Zonen und LPARs werden nur grundlegend unterstützt. Es werden keine zusätzlichen Inventardaten über die Umgebung (z. B. Gast-Host-Zuordnung) erfasst und die Ausführung in untergeordneten Zonen wird nicht unterstützt.

[14] Unterstützung von Software-Erkennungsregel unter OS X in Version 7.5.

[15] Ab Version 10.8 nennt Apple sein Betriebssystem nicht mehr Mac OS X, sondern nur OS X.

[16] Zum Zeitpunkt der Veröffentlichung dieser Version dieses Dokuments war OS X Server 10.9 noch nicht verfügbar. Die Veröffentlichung ist für Herbst 2013 geplant.

Deployment Solution

Dieser Abschnitt umfasst Deployment Solution (DS) 6.9 SP6 und unterscheidet sich von den übrigen Tabellen in diesem Dokument. Für DS gibt es zwei verschiedene Typen von Betriebssystemunterstützung. 1) Imaging-Unterstützung: Für das Betriebssystem ist Imaging mit DS möglich. 2) Unterstützung für skriptgesteuerte Betriebssysteminstallation: Das Betriebssystem kann auf einem

Computer durch eine skriptgesteuerte Betriebssysteminstallation (SOI) bereitgestellt werden. Die folgende Tabelle beschreibt die Betriebssystemunterstützung für DS[1,2].

Tabelle A-13 Imaging Betriebssystem Stützmatrix

Imaging-Unterstützung	6.9 SP5 MR3	7.2 SP2 MP1.1	6.9 SP6	7.5
Windows XP				
Windows XP Professional SP2 x86/x64	Nicht unterstützt	Unterstützt	Nicht unterstützt	Produkteinstellung
Windows XP Professional SP3 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Vista				
Windows Vista x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Vista SP1 x86/x64	Nicht unterstützt	Unterstützt	Nicht unterstützt	Produkteinstellung
Windows Vista SP2 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows 7				
Windows 7 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows 7 SP1 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows 7 SP2 x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows 8				
Windows 8	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]	Unterstützt	Unterstützt
Apple OS X				
Apple Mac OS X (10.4) Universal	Begrenzte Unterstützung[6]	Nicht unterstützt	Begrenzte Unterstützung [6]	Nicht unterstützt
Apple Mac OS X (10.5) Universal	Begrenzte Unterstützung[6]	Nicht unterstützt	Begrenzte Unterstützung [6]	Nicht unterstützt

Imaging-Unterstützung	6.9 SP5 MR3	7.2 SP2 MP1.1	6.9 SP6	7.5
Apple Mac OS X (10.6)	Begrenzte Unterstützung[6]	Nicht unterstützt	Begrenzte Unterstützung [6]	Unterstützt
Apple Mac OS X (10.7)	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt
Apple OS X (10.8)	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt
Apple OS X (10.9)[7]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Server 2003				
Windows Server 2003 SP2 x86	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2003 SP2 x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2003 SP2 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008				
Windows Server 2008 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server SP2 2008 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 Core x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R2	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R2 Core	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R1 SP2	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R2 SP2	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Server 2012				
Windows Server 2012	Begrenzte Unterstützung [5]	Begrenzte Unterstützung [5]	Unterstützt	Unterstützt

Imaging-Unterstützung	6.9 SP5 MR3	7.2 SP2 MP1.1	6.9 SP6	7.5
Red Hat Enterprise Linux 4				
Red Hat Enterprise Linux 4 ES x86	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Red Hat Enterprise Linux 4 AS x86	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Red Hat Enterprise Linux 5				
Red Hat Enterprise Linux 5 Server x86	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Red Hat Enterprise Linux 5.1 Server x86	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Red Hat Enterprise Linux 5.2 Server x86	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Red Hat Enterprise Linux 5.3 Server x86	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Red Hat Enterprise Linux 5.4 Server x86	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Red Hat Enterprise Linux 5.5 Server x86	Unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Red Hat Enterprise Linux 5.6 Server x86	Unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Red Hat Enterprise Linux 5.7 Server x86	Unterstützt	Nicht unterstützt	Unterstützt	Nicht unterstützt
Red Hat Enterprise Linux 5.8 Server x86	Unterstützt	Nicht unterstützt	Unterstützt	Nicht unterstützt
Red Hat Enterprise Linux 5.9 Server x86	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Red Hat Enterprise Linux 6[4]				
Red Hat Enterprise Linux 6.0 x86	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt
Red Hat Enterprise Linux 6.1 x86	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt

Imaging-Unterstützung	6.9 SP5 MR3	7.2 SP2 MP1.1	6.9 SP6	7.5
Red Hat Enterprise Linux 6.2 x86	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt
Red Hat Enterprise Linux 6.3 x86	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt
Red Hat Enterprise Linux 6.4 x86	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Novell SUSE Linux Enterprise Server				
Novell SUSE Linux Enterprise Server 9 x86	Unterstützt	Nicht unterstützt	Unterstützt	Nicht unterstützt
Novell SUSE Linux Enterprise Server 10 x86	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Novell SUSE Linux Enterprise Server 11 x86	Unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Novell SUSE Linux Enterprise Server 12 x86	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

[1] Deployment Solution 7 wird auf der Symantec Management-Plattform erstellt und basiert auf DS 6.9, einer eigenständigen Windows-Anwendung.

[2] Weitere Informationen zu Deployment Solution 6.9 (einschließlich Systemanforderungen) erhalten Sie im folgenden Artikel:

http://www.symantec.com/docs/DOC2079

[4] Sofern nicht anders angegeben, gilt dies für Server-, Client- und Arbeitsstationversionen des Betriebssystems.

[5] Begrenzter Support wurde für diese Versionen eingeführt. Weitere Informationen erhalten Sie auf den folgenden Webseiten:

http://www.symantec.com/docs/DOC6284 und

http://www.symantec.com/docs/DOC6299

[6] DS 6.9 erfordert Mac OS X Server für Mac-Imaging.

[7]Zum Zeitpunkt dieses Releases ist OS X Server 10.9 (Mavericks) noch nicht veröffentlicht. Das Release ist für Herbst 2013 geplant.

Tabelle A-14 Matrix der Unterstützung für skriptgesteuerte Betriebssysteminstallation

Unterstützung für skriptgesteuerte Betriebssysteminstallation	6.9 SP5 MR3	7.1 SP2 MP1.1	6.9 SP6	7.5
Windows XP				
Windows XP Professional SP2 x86/x64	Unterstützt	Unterstützt	Unterstützt	Produkteinstellung
Windows XP Professional SP3 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Vista				
Windows Vista x86/x64	Unterstützt	Nicht unterstützt	Unterstützt	Nicht unterstützt
Windows Vista SP1 x86/x64	Unterstützt	Unterstützt	Unterstützt	Produkteinstellung
Windows Vista SP2 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows 7				
Windows 7 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows 7 SP1 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows 7 SP2 x86/x64	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows 8				
Windows 8	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt
Apple OS X				
Apple Mac OS X (10.6)	Begrenzte Unterstützung [5]	Nicht unterstützt	Begrenzte Unterstützung [5]	Unterstützt[6]
Apple Mac OS X (10.7)	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt[6]
Apple OS X (10.8)	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt[6]

Unterstützung für skriptgesteuerte Betriebssysteminstallation	**6.9 SP5 MR3**	**7.1 SP2 MP1.1**	**6.9 SP6**	**7.5**
Apple OS X (10.9)[7]	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Server 2003				
Windows Server 2003 SP2 x86	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2003 SP2 x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2003 R2 SP2 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008				
Windows Server 2008 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server SP2 2008 x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 Core x86/x64	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R2	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R2 Core	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R1 SP2	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R2 SP2	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows Server 2012				
Windows Server 2012	Eingeschränkte Unterstützung [1]	Eingeschränkte Unterstützung [2]	Unterstützt	Unterstützt
Red Hat Enterprise Linux 4				
Red Hat Enterprise Linux 4 ES	Unterstützt	Unterstützt	Unterstützt	Unterstützt

Unterstützung für skriptgesteuerte Betriebssysteminstallation	**6.9 SP5 MR3**	**7.1 SP2 MP1.1**	**6.9 SP6**	**7.5**
Red Hat Enterprise Linux 4 AS	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Red Hat Enterprise Linux 5				
Red Hat Enterprise Linux 5 Server	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Red Hat Enterprise Linux 5.1 Server	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Red Hat Enterprise Linux 5.2 Server	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Red Hat Enterprise Linux 5.3 Server	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Red Hat Enterprise Linux 5.4 Server	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Red Hat Enterprise Linux 5.5 Server	Unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Red Hat Enterprise Linux 5.6 Server	Unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Red Hat Enterprise Linux 5.7 Server	Unterstützt	Nicht unterstützt	Unterstützt	Nicht unterstützt
Red Hat Enterprise Linux 5.8 Server	Unterstützt	Nicht unterstützt	Unterstützt	Nicht unterstützt
Red Hat Enterprise Linux 5.9 Server	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Red Hat Enterprise Linux 6				
Red Hat Enterprise Linux 6.0	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt
Red Hat Enterprise Linux 6.1	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Unterstützt
Red Hat Enterprise Linux 6.2	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

Unterstützung für skriptgesteuerte Betriebssysteminstallation	6.9 SP5 MR3	7.1 SP2 MP1.1	6.9 SP6	7.5
Red Hat Enterprise Linux 6.3	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Red Hat Enterprise Linux 6.4	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Novell SUSE Linux Enterprise Server				
Novell SUSE Linux Enterprise Server 9	Unterstützt	Nicht unterstützt	Unterstützt	Nicht unterstützt
Novell SUSE Linux Enterprise Server 10	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Novell SUSE Linux Enterprise Server 11	Unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Novell SUSE Linux Enterprise Server 12	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
VMware ESX/ESXi				
VMware ESX 3.5	Eingeschränkte Unterstützung[4]	Nicht unterstützt	Eingeschränkte Unterstützung[4]	Nicht unterstützt
VMware ESX/ESXi 4.x	Eingeschränkte Unterstützung[4]	Nicht unterstützt	Eingeschränkte Unterstützung[4]	Eingeschränkte Unterstützung[4]
VMware ESXi 5.1	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Eingeschränkte Unterstützung[4]

[1] Eingeschränkte Unterstützung wurde für DS 6.9 SP5 MR3 eingeführt. Weitere Informationen erhalten Sie im folgenden Supportdatenbank-Artikel:

http://www.symantec.com/docs/DOC6299

[2] Eingeschränkte Unterstützung wurde für DS 7.1 SP2 MP1.1 eingeführt. Weitere Informationen erhalten Sie im folgenden Supportdatenbank-Artikel:

http://www.symantec.com/docs/DOC6284

[4] Dies ist nur auf die Bereitstellung des VMware-Host-Betriebssystems beschränkt und bezieht sich nicht auf die SOI der Gast-Betriebssysteme.

[5] DS 6.9 erfordert Mac OS X Server für Mac-Imaging.

[6] In DS 7.5 werden skriptgesteuerte OS-Installation als NetInstall bezeichnet.

[7]Zum Zeitpunkt dieses Releases ist OS X Server 10.9 noch nicht veröffentlicht. Das Release ist für Herbst 2013 geplant.

Sprachunterstützung

Der folgende Abschnitt enthält die Sprachunterstützung für Symantecs IT Management Suite für die Core-Plattform und den Management Agent.

Core-Lokalisierung gibt an, dass die Konsolen- und Hilfedateien in den referenzierten Sprachen lokalisiert wurden. Sie gibt auch die unterstützte Sprache für das Betriebssystem an, unter dem der Notification Server installiert ist.

"Agent lokalisiert" gibt an, dass Agent und Agent-Hilfe in die angegebenen Sprachen übersetzt wurden.

Core-Lokalisierung

Tabelle A-15 Core-Lokalisierung

Core-Lokalisierung	6.x	7.0 SP5	7.1 SP2 MP1.1	7.5
Englisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Deutsch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Französisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Japanisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Spanisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Chinese (vereinfacht)	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Italienisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Russisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Portugiesisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Koreanisch	Nicht unterstützt	Unterstützt	Unterstützt	Unterstützt
Chinese (traditionell)	Nicht unterstützt	Unterstützt	Unterstützt	Unterstützt

Windows-Agent-Lokalisierung

Tabelle A-16 Windows-Agent-Lokalisierung

Core-Lokalisierung	6.x	7.0 SP5	7.1 SP2 MP1.1	7.5
Englisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Deutsch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Französisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Japanisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Spanisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Chinese (vereinfacht)	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Italienisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Russisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Portugiese (Brasilien)	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Schwedisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Dänisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Finnisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Polnisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Norwegisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Niederländisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Koreanisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Chinese (traditionell)	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Türkisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Tschechisch	Unterstützt	Unterstützt	Unterstützt	Unterstützt

Index

A

Agent
  Optimierung 113
Agent-basierte Inventarisierung 87
Agent-Vertrauen
  aufbauen 61
  Info zu 61
Aktualisierungszeitplan fertig stellen
  Konfigurieren 111
Application Metering 90
Application Metering-Inventardaten 90
Arbeitsspeicher
  SQL Server 43
Architektur
  Planung 37
  Symantec Management-Plattform 22
Asset Management
  Datenfluss 99

B

Basisinventardaten 91
Basisinventarisierung 91
Benutzerdefinierte Inventardaten 89
Benutzerdefinierte Inventarisierung 89
Berichte
  MultiCMDB 128

C

Cloud-fähige Verwaltung
  Info zu 31
CMDB
  Arbeitsspeicher 43
  Datenträgerkonfiguration 41
  Größe 42

D

Datenträgerkonfiguration
  SQL Server 41
Delta-Aktualisierungszeitplan
  Konfigurieren 111
Dokumentation 18
Duplizieren
  Richtlinien 110

F

Failover 46
Filter
  Mitgliedschaftsaktualisierungen planen 111
Flash
  Anforderungen 75

G

Grundinventardaten 86
Grundinventarisierung 86

H

Hardware
  IT Management 62
Hardwareempfehlungen
  Internet-Gateway 66
  Notification Server 62, 67
  Package Server 62
  SQL Server 62
  Task Server 62
Hierarchie
  Einrichten 124
  Site Server 121
  Topologie 120
Hierarchiereplikation
  Einsatzmöglichkeiten 120
  Einschränkungen 122
  Info zu 118
  Überlegungen zu Patch Management 122
  Überlegungen zu Software Management 121
Hilfe
  Kontextbezogen 18

I

IIS Rollen-Dienste
  benötigt 73

Internet-Gateway
Hardwareempfehlungen 66
Inventar
Datenfluss 78
Planen 110
Inventardaten
Erfassungsmethoden 86
Inventarisierung
Methoden 86
Inventarisierungsleistung
Info 81
Optimierung 81
Inventarisierungsrichtlinien 110
Duplizieren 110
Inventory für Netzwerkgeräte 92
IT Management
Funktionen 12
Hardware 62
Info 11
Verhältnis von Komponenten 68
Verständnis 13

J
Java
Anforderungen 76

K
Konsole
Leistung 116
Kontextbezogene Hilfe 18

L
Leistung
Konsole 116
Leistungsoptimierung
Agent 113
Einstellungen 115
Faktoren 108
NSE 109
Lösungen
IT Management Suite 24

M
Microsoft Access 2010
OLEDB-Treiber 75
MultiCMDB
Berichte 128

N
Netzwerkstartserver
Info zu 58
Notification Server
Betriebssystemanforderungen 69
Hardwareempfehlungen 62, 67
Überblick 23
NSE
Leistungseinschränkungen 109
Nutzungsverfolgungsdaten 90

O
OLEDB-Treiber
Microsoft Access 2010 75
Organisationsgruppe
Zeitplan aktualisieren 111

P
Package Server
Betriebssysteme, unterstützt 70
Hardwareempfehlungen 62
Package Service
Info 57
Patch-Management
Datenfluss 95
Planung
IT-Verwaltung 37
PXE-Server
Info zu 58

R
Replikation
Regeln 126
Typen 117
Ressourcen
geplante Filteraktualisierungen 111
Richtlinien
Duplizieren 110
Inventar 110
Richtlinienaktualisierungszeitplan
Konfigurieren 111

S
Silverlight
Anforderungen 76
Site Server
Aufgabe 53

Betriebssystemanforderungen 69
Info 57
Netzwerkstartserver 58
Planung 51
Überlegungen zur Hierarchie 121
Software Management Framework
Info 23
Software, Drittanbieter
Anforderungen 75
Softwarenutzungsverfolgung 90
Sortierungen, SQL
unterstützt für IT Management Suite 72
SQL Server
Arbeitsspeicher 43
Datenträgerkonfiguration 41
Empfehlungen 75
Größe 42
Hardwareempfehlungen 62
Kollatierungen, unterstützt 72
Konfiguration planen 39
SQL Server-Failover 46
Standalone-Inventarisierung 88
Standardinventardaten 87
Standort
Site Server 52
Standortwartung 52
Symantec Management Agent
in Image einbetten 60
Symantec Management-Plattform
Architektur 22
Einleitung 21
Info 21, 23
Komponenten 23
Systemanforderungen
IIS Rollen-Dienste 73

T

Task Server
Betriebssysteme, unterstützt 70
Hardwareempfehlungen 62
Tickle 55
Task Service
Info 53
Tickle
Task Server 55

V

Versionshinweise 18
Verweigern von Anwendungen 90

Z

Zeitplan
Ressourcen-Mitgliedschaftsaktualisierungen 111
Ziel
Zeitplan aktualisieren 111